CHAPITRE 7

LA PRATIQUE DE LA PROTECTION DU SECRET

Si dans l'évolution du contexte juridique des activités de contre-espionnage, le secret de la défense nationale a perdu la place centrale qu'il y occupait, il n'en demeure pas moins que la préservation de ce secret par des mesures préventives et la répression de ses éventuelles compromissions ont toujours été, depuis l'origine, des aspects essentiels de l'activité de contre-espionnage. Le système actuellement opérationnel repose sur le décret du 17 juillet 1998 relatif à la protection des secrets de la défense nationale. Il comporte deux volets essentiels : la classification des informations et supports d'information et l'habilitation des personnes, complétés par ailleurs par des dispositions relatives à la protection physique des sites.

LA CLASSIFICATION DES INFORMATIONS

Les informations pouvant relever du secret de défense sont d'abord protégées au travers de leurs supports : document imprimé ou sur support informatique, voire – dans certains cas – des objets (des prototypes, par exemple). La mesure de protection applicable aux informations secrètes et à leurs supports est la « classification ».

Les différents niveaux de classification

La définition réglementaire des niveaux de classification

Ainsi que nous l'avons déjà indiqué, c'est le décret du 12 mai 1981 qui donna un fondement réglementaire à la protection du secret et, en particulier à la procédure de classification des informations, en décrétant dans son article 2 que

« les renseignements, objets, documents, procédés intéressant la défense nationale et la sûreté de l'État qui doivent être tenus secrets font l'objet

d'une classification comprenant trois niveaux de protection : Très Secret-Défense, Secret-Défense et Confidentiel-Défense. » [1]

Il définissait ensuite les caractéristiques de chacune de ces trois catégories :

– la mention *Très Secret-Défense* (article 4) était réservée *« aux informations dont la divulgation est de nature à nuire à la défense nationale et à la sûreté de l'État et qui concernent les priorités gouvernementales en matière de défense »* ;

– la mention *Secret-Défense* (article 5 premier alinéa) était réservée *« aux informations dont la divulgation est de nature à nuire à la défense nationale et à la sûreté de l'État »* ;

– la mention *Confidentiel-Défense* recouvrait les *« informations qui ne présentent pas en elles-mêmes un caractère secret mais dont la connaissance, la réunion ou l'exploitation peuvent conduire à la divulgation d'un secret intéressant la défense nationale ou la sûreté de l'État »* (article 5 alinéa 2).

Le décret du 17 juillet 1998 qui a abrogé et remplacé le décret de 1981 a conservé cette même hiérarchie du secret de défense en trois catégories [2]. Mais il a, sur certains aspects, modifié la définition des classifications et s'est efforcé d'adapter le système préventif à la nouvelle réalité juridique découlant du nouveau code pénal de 1994.

S'agissant du niveau *Très Secret-Défense*, l'article 3 précise qu'il est réservé *« aux informations ou supports protégés dont la divulgation est de nature à nuire gravement à la défense nationale et qui concernent les priorités gouvernementales en matière de défense »*. Cette dualité de critère existait déjà depuis 1981, mais jusqu'alors s'il fallait que les informations en question touchent bien aux priorités en matière de défense, il suffisait que leur divulgation soit *« de nature à nuire à la défense »*. Ajouté en 1998, l'adverbe *« gravement »* indique un renforcement de l'exigence requise, et donc – indirectement – une restriction à l'usage de cette haute classification. Si, en effet, il est difficile de ne pas considérer que toute information concernant une priorité gouvernementale en matière de défense peut nuire, par sa divulgation, à cette même défense, il est désormais exigé de l'autorité administrative qu'elle ne protège à ce niveau que celles qui pourraient occasionner une nuisance particulière.

On retrouve la même évolution par rapport à 1981 en ce qui concerne le *Secret-Défense*. À ce niveau, la modification est tout à fait similaire à celle effectuée pour le *Très Secret-Défense*. Le niveau *Secret-Défense « est réservé aux informations ou supports protégés dont la divulgation est de nature à nuire gravement à la défense nationale »* (art. 3, alinéa 2). La différence entre les deux niveaux demeure, comme en 1981, le lien pouvant exister – ou non – avec une priorité gouvernementale de défense. Tout au plus, l'adjonction de l'adverbe *« gravement »* rend également plus sévère les conditions d'accès au niveau *Secret-Défense*.

En revanche, la définition du *Confidentiel-Défense* change assez profondément. Dans l'esprit de 1981 (et des instructions d'application non

---

[1] Décret n° 81-514 du 12 mai 1981 relatif à l'organisation de la protection des secrets et des informations concernant la défense nationale et la sûreté de l'État, *JORF*, 15 mai 1981.

[2] Décret n° 98-608 du 17 juillet 1998 relatif à la protection des secrets de la défense nationale, *JORF*, 19 juillet 1998, p. 11118.

publiées), ce niveau CD ne constituait pas un véritable niveau de secret mais uniquement un instrument de protection périphérique des véritables secrets (qui pouvaient se trouver indirectement compromis par la révélation du contenu du document *Confidentiel-Défense*). Pour autant, cette définition minimale débouchait sur une grande hypocrisie administrative et juridique, puisqu'un document CD était pratiquement considéré comme un secret à part entière et sa que violation était susceptible d'entraîner le même type de sanction pénale. C'est sans doute pourquoi le troisième alinéa de l'article 3 n'affirme plus que, par principe, les informations classifiées au niveau *Confidentiel-Défense* ne sont pas des secrets, mais – au contraire – les définit comme des *« informations ou supports protégés »* dont la divulgation serait de *« nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de défense classifié au niveau Très Secret-Défense ou Secret-Défense. »*

Cette nouvelle formulation donne ainsi bien au *Confidentiel-Défense* toute sa dignité et toute son importance [3]. Dans la mesure où il couvre explicitement des *« informations ou supports protégés »* (définis comme des secrets de la défense nationale, dans l'article 1er), il ne peut être mis en œuvre que pour couvrir de véritables secrets de défense, qui peuvent être de deux sortes : soit des secrets en eux-mêmes suffisamment sensibles pour que leur divulgation nuise à la défense, soit ce que la doctrine traditionnelle appelle souvent des *« secrets par extension »*.

Là encore, cette redéfinition du *Confidentiel-Défense* va dans le sens d'un durcissement des conditions de classification des informations puisque sous l'ancien régime du décret de 1981, l'ambiguïté du texte laissait une certaine latitude à l'administration pour couvrir de toutes les contraintes administratives et juridiques du secret, des informations qui n'en étaient pas réellement. Autrement dit, la rédaction du décret de 1981 permettait de fabriquer, grâce à la classification CD, ce que l'on pouvait ironiquement considéré comme des « vrais-faux » secrets de défense, et encourageait ainsi à l'abus de la sur-classification. Au contraire, le nouveau *Confidentiel-Défense* est désormais un secret de défense comme les autres qui doit pouvoir justifier, notamment aux yeux de la justice, de sa consistance et des risques que sa divulgation ferait courir – directement ou indirectement – à la défense nationale.

La définition de ces catégories partage le même esprit mais ne correspond pas toujours exactement aux classifications en vigueur dans d'autres pays occidentaux [4]. Prenons, à titre d'exemple, les définitions des classifications homologues existant aux Etats-Unis, telles qu'elles résultent de l'Executive Order n° 12958 :

– *« Top Secret »* est réservé aux informations dont *« on peut raisonnablement penser que la divulgation non autorisée causerait un dommage*

---

[3] Parlant du *Confidentiel-Défense*, on pouvait encore écrire avant la réforme du nouveau Code pénal que *« de même qu'il existe des « délits-obstacles », tel le port d'arme, qui ont pour objet d'éviter la commission d'infractions plus graves, le niveau Confidentiel-Défense peut être assimilé à une « classification-obstacle » pour l'accès à des secrets de défense »* (Robert Blaser, « Le secret de défense », *Défense nationale*, mars 1990, p. 82).

[4] Un tableau comparatif des niveaux de classifications dans les différents États membres de l'OTAN a été publié, en annexe de l'accord OTAN sur le secret des inventions intéressant la défense (cf. décret n° 65-234 du 26 mars 1965, *JORF*, 1er avril 1965, p. 2565). Pour un tableau

grave et exceptionnel à la sécurité nationale que l'autorité responsable de la classification originelle est en mesure d'identifier ou de décrire » ;

– la mention *« Secret »* s'applique à des informations dont la divulgation ne pourrait causer qu'un *« sérieux dommage »* à la sécurité nationale ;

– la mention *« Confidential »* concerne, pour sa part, les informations dont la divulgation pourrait causer *« un dommage »* à la sécurité nationale.

Le principe à la base de cette décomposition est bien un principe *« finaliste »*, c'est-à-dire que – comme dans le système français – c'est le danger que représenterait *a posteriori* la divulgation de l'information qui détermine sa classification *a priori*. On y retrouve également le caractère quelque peu subjectif de l'appréciation de l'importance des dommages.

Les critères de détermination des niveaux de classification

Ces définitions qui cherchent à distinguer les différents niveaux de secret ne sont pas exempts de toute critique, tant les critères qui servent réellement à l'autorité administrative pour classifier apparaissent souvent comme obscurs [5]. Bien que ces critères ne soient pas généralement publiés, plusieurs auteurs nous donnent, néanmoins, des indications à ce sujet.

Il semble, qu'à l'origine, la différenciation s'effectuait surtout en fonction de l'ampleur de la diffusion que l'autorité émettrice entendait donner au document :

> *« La classification « Confidentiel » comporte une distribution limitée, mais qui peut encore être assez ample. Les documents catalogués « Secrets » peuvent encore atteindre plusieurs centaines d'ayants droit, mais les « Très Secrets » sont vus seulement par un nombre de gens très restreints, ne dépassant pas souvent deux ou trois. »* [6]

Mais, ce critère de la diffusion – logiquement dominant en période de conflit ou de crise (dans lesquelles la sécurité est un impératif absolu) – n'est plus aujourd'hui la raison prioritaire du choix d'un niveau de classification (il en serait plutôt la conséquence [7]). D'autres critères sont généralement pris en compte, de nature interne ou externe à l'information concernée. Ainsi, par exemple, plusieurs éléments génériques seraient prioritairement pris en compte par le SGDN [8] :

– l'importance et la finalité du document dans l'organisation et la politique de défense ;

---

comparatif (non officiel) plus récent et plus complet, cf. Jacques Baud, *Encyclopédie du renseignement et des services secrets*, Lavauzelle, 1997, pp. 104-105.

[5] *« La frontière entre les espaces du secret est obscure – pourquoi telle information sera classifiée et telle autre non ? pourquoi la classer dans telle ou telle catégorie ? pourquoi telle information sera-t-elle, un jour, déclassifiée ? comment distinguer ce qui relève de la « priorité » gouvernementale ? – et hétérogène, du fait de la multiplicité des critères »* (Alain Dewerpe, *Espion – Une anthropologie historique du secret d'État contemporain*, Gallimard, 1994, p. 140).

[6] Ladislas Farago, *War of Wits*, traduction française : *Les secrets de l'espionnage*, Presses de la Cité, 1955, p. 114.

[7] Les fonctionnaires engagés dans la protection du secret reconnaissent cependant que l'interaction continue à jouer dans les deux sens, comme le précise ce magistrat, alors chef du bureau réglementation au SSD : *« il existe une espèce d'effet rétroactif des contraintes de la protection sur le choix du niveau de classification : il faut s'assurer que l'usage et la diffusion pressentis de l'information sont compatibles avec les mesures de protection imposées par ce niveau. A défaut, il faut se donner les moyens de respecter ces mesures ou renoncer au niveau de classification projeté »* (R. Blaser, *op. cit.*, p. 83).

[8] Pierre Péan, *Secret d'État – La France du secret, les secrets de la France*, Fayard, 1986, p. 42.

– la protection des sources de l'information contenue dans le document [9] ;

– le degré de sensibilité à l'égard de l'opinion publique ;

– l'importance de l'information aux regards des différents intérêts vitaux de la nation.

Plutôt que ces critères internes (c'est-à-dire qui déterminent le niveau de secret à partir de la situation française), un ancien officier supérieur de la DPSD préfère mettre en avant

> *« l'intérêt, donc l'attrait que présente la connaissance de l'information considérée pour autrui et tout spécialement pour une puissance ou une organisation étrangère. C'est, par conséquent, l'intensité de cet attrait qui fixera le degré de la protection à assurer, en fonction, bien entendu, du préjudice que sa compromission ferait subir à la nation. »* [10]

Dans le même sens, une commission du Sénat américain a retenu comme objectif essentiel de toute classification de s'assurer qu'*« un agent hostile dont le but est de porter atteinte aux intérêts des Etats-Unis ne pourra pas utiliser l'information. »* [11]

Ce critère externe (qui privilégie le point de vue de l'adversaire) n'est pas nouveau et à toujours été utilisé dans le domaine strictement militaire. Ainsi, pouvait-on lire, il y a plus de trente ans dans la *Revue militaire d'information* qu'une information ne doit devenir un secret militaire que si trois conditions sont remplies :

> *« Si l'ennemi peut les percevoir par un moyen quelconque* (...) *Si l'ennemi peut en déduire un enseignement intéressant quant à nos possibilités ou à nos intentions* (...) *Si l'ennemi peut utiliser cet enseignement. »* [12]

C'est aussi l'avis plus récent d'un spécialiste du contre-espionnage qui estime que *« les règles de classification mettent en avant l'importance du secret dans notre propre système de défense. Il est pourtant évident que c'est la valeur attachée à ce secret par l'adversaire qui compte. »* [13]

Les classifications spéciales « Très secret-défense »

En ce qui concerne les informations de niveau *Très Secret-Défense*, elles sont réparties, suivant leur objet, entre plusieurs *« classifications spéciales »* définies et gérées directement par le Service de sécurité de

---

[9] La protection des sources clandestines est l'un des motifs les plus fréquemment invoqués pour justifier la classification d'information (*« Pour tout service de renseignement, la protection de ses sources secrètes est un dogme »*, Amiral Pierre Lacoste, « Du renseignement et des hommes », *Défense nationale*, octobre 1994, p. 45). C'est particulièrement vrai en matière d'informations obtenues par voie d'interception (écoutes, décryptement de messages chiffrés) : la simple connaissance du fait qu'une information est connue d'un tiers peut permettre d'identifier la source de la fuite (par exemple, comprendre que les liaisons sont écoutées ou que le code est « cassé »).

[10] Henri Debrun, « Le secret de défense » in Jacques Robert (sous la dir.) *L'esprit de défense*, Economica, 1987, Debrun, *op. cit.*, p. 444.

[11] Senate Select Committee on Intelligence, *Meeting the Espionage Challenge : A Review of United States Counterintelligence and Security Programs*, 99th Cong., 2d sess., 1986, Rpt. 99-522, 78.

[12] Colonel Achard-James, « La conservation du secret militaire », *Revue militaire d'information*, n° 171, 10 avril 1951, p. 25.

[13] Cité par P. Péan, *op. cit.*, p. 42.

défense du SGDN, pour le compte du Premier ministre. Le décret du 17 juillet 1998 indique, en effet, que *« le Premier ministre définit les critères et les modalités d'organisation de la protection des informations ou supports protégés au niveau Très secret défense »* (article 5, 1er alinéa), qu'il *« définit les classifications spéciales dont ils font l'objet et qui correspondent aux différentes priorités gouvernementales »* (article 5, alinéa 2) et qu'il *« indique notamment la ou les catégories spéciales auxquelles la personne habilitée* [au Très Secret-Défense] *a accès »* (article 8, 2e alinéa).

On compte notamment parmi ces classifications spéciales :

– la classification *« Très secret Rubis »*, qui couvre les informations relatives à l'emploi des forces nucléaires stratégiques [14] ;

– la classification *« Très secret Diamant »*, pour la protection des informations très secrètes du renseignement ;

– la classification *« Très secret Conseil »*, pour la protection des informations très secrètes traitées lors des Conseils de défense et des comités interministériels qui s'y rapportent [15] ;

– la classification *« Très secret Megal »*, pour la protection des informations très secrètes du *« mémento général »* [16].

Pierre Péan signale, pour sa part, l'existence – outre d'un *« Très secret Cosmic »* (couvrant les informations très secrètes de provenance OTAN – cf. infra) d'un *« Très secret Habile »* et d'un *« Très secret Olifant »* (sans donner de précisions sur leur contenu) [17].

La particularité de toutes ces classifications spéciales est leur cloisonnement entre elles [18] : on accède à chacune d'entre elles par une procédure

---

[14] J.-J. Rodilla signale qu'il s'agit de la plus ancienne des classifications spéciales et qu'elle a été *« instituée par l'instruction particulière du Premier ministre n° 1515/DN/SD du 10 juin 1964 »* (J.-J. Rodilla, *Protection du secret de la défense nationale*, mémoire DESS, Université de Nice, 1979, annexe 5) ce qui nous amène à comprendre que ces *« classifications spéciales »* sont apparues en France sous la Ve République, consécutivement à la modification du système de protection du secret qui a suivie l'ordonnance de 1960 et à la mise en place des forces stratégiques.

[15] Cf. P. Péan, *op. cit.*, pp. 53 à 55; Cf. Jean Guisnel & Bernard Violet, *Services secrets - Le pouvoir et les services de renseignement sous François Mitterrand*, La Découverte, 1988, p. 234; A. Dewerpe, *op. cit.*, p. 140.

[16] Le *« mémento général »* est le document rassemblant, au niveau national, l'ensemble des mesures à prendre pour assurer – en cas de crise ou d'agression – la défense des *« points sensibles »* du territoire (sur cette notion, cf. infra). Il existe également certains mémentos particuliers destinés aux ministères les plus importants. Tous ces documents sont fortement classifiés (cf. P. Péan, *op. cit.*, p. 146).

[17] Cf. P. Péan, *op. cit.*, p. 52.

[18] Le système de classifications spéciales – issu du système de protection mis au point par les alliés pour protéger les décryptements des messages allemands et japonais – est très pratiqué aux États-Unis. Il existerait une trentaine de classifications *« Sensitive Compartmented Intelligence »* (SCI), dont la particularité est de combiner *« un cloisonnement vertical et un cloisonnement horizontal de l'information (classification matricielle). Le principe en est d'autoriser (respectivement de limiter) l'accès à certains projets, et à l'information à l'intérieur de ces projets »* (J. Baud, *op. cit.*, p. 106). Les personnes qui y sont habilitées sont dites *« bigot »*, vieux terme déjà utilisé pour désigner les rares initiés connaissant les secrets du débarquement allié en Normandie en 1944. Mais ce système peut occasionner un cloisonnement et des malentendus bureaucratiques préjudiciables comme en témoigne l'Amiral Turner (directeur de la CIA de 1977 à 1981) : *« La première règle pour tous les noms de code est que vous ne pouvez discuter des informations contenues dans un document portant un code donné avec quiconque n'a pas reçu l'autorisation d'accès à ce type de code. À mon niveau de responsabilité, je pouvais généralement compter sur mon équipe pour s'assurer que je n'évoquais les différents sujets qu'avec les personnes correctement habilitées pour traiter de chacune de ces catégories de sujets classifiés. Mais ce qui m'ennuyait, c'est que, comme le système était difficile à comprendre, d'autres qui n'avaient pas le soutien dont*

d'habilitation séparée gérée par le SGDN, ce qui fait qu'une personne habilitée à l'une des classifications *Très secret* n'a aucun droit à accéder aux documents relevant d'une autre. De plus, chacune de ces classifications est gérée physiquement par une structure autonome [19].

Les classifications interalliées

Parallèlement aux trois mentions de classification établis par le décret du 12 mai 1981, existent en France – comme dans les autres États signataires du Traité de l'Atlantique Nord – les classifications OTAN. De même, la France étant membre de l'Union de l'Europe Occidentale, respecte les classifications UEO.

Une instruction interministérielle n° 2100 du SGDN en date du 1er décembre 1975 (non publiée) régit l'application en France du système de sécurité applicable aux informations OTAN [20]. Ce système comporte trois niveaux de classification homologues des niveaux français, mais d'une définition identique à celle des classifications américaines :

– Cosmic Très Secret *(Cosmic Top Secret)* : *« Cette catégorie de classification sera uniquement appliquée aux renseignements dont la divulgation non autorisée aurait des conséquences exceptionnellement graves pour l'Organisation du Traité de l'Atlantique Nord ».*

– NATO Secret : *« Cette catégorie de classification sera uniquement appliquée aux renseignements dont la divulgation non autorisée aurait des conséquences graves pour l'OTAN ».*

– NATO Confidentiel *(NATO Confidential)* : *« Cette catégorie de classification sera uniquement appliquée aux renseignements dont la divulgation non autorisée serait préjudiciable aux intérêts de l'OTAN »* [21].

Au sein de l'UEO, un système équivalent existe avec les trois niveaux suivants : *Focal Top Secret, WEU Secret, WEU Confidential* (et leurs homologues en langue française) [22]. L'application en France du système

---

je disposais ne devaient pas respecter correctement les règles. Les racines de ce problème, comme je l'ai découvert, venait du fait que le nombre de noms de code avait proliféré aussi rapidement que les nouveaux systèmes technologiques. Les codes se superposaient; et même lorsqu'ils émanaient de la même agence, il y avait de fortes duplications » (Stanfield Turner, *Secrecy and Democraty – The CIA in Transition*, Houghton Mifflin Company, Boston, 1985, p. 255).

[19] *« Afin de protéger, en quelque sorte, les utilisateurs contre eux-mêmes (ils sont rarement des spécialistes de la sécurité), on va doubler ce réseau d'utilisation d'un réseau de sécurité (composé, lui, de professionnels) par lequel transiteront obligatoirement toutes les informations circulant entre les utilisateurs. Enfin, on installera au centre de ce réseau, tel le moyeu d'une roue, un service chargé de rassembler tous les signalements d'émission, de circulation et de destruction des documents classifiés, afin d'en connaître à chaque instant les détenteurs mais jamais leur contenu »* (R. Blaser, *op. cit.*, p. 85).

[20] Cf. Alain-Louis Mie, *L'administration et le droit à l'information*, Berger-Levrault, 1985, pp. 157 et 185. Du fait, sans doute, de la non-participation de la France à l'organisation militaire intégrée de l'OTAN, il semble que les documents classifiés OTAN à haut niveau soient très peu nombreux en France : d'après le ministre de la défense, Alain Richard, une dizaine de documents au niveau Secret OTAN par an (cf. Assemblée nationale, 1re séance du 12 février 1998, *Compte rendu analytique officiel*, p. 15).

[21] Décret n° 65-234 du 26 mars 1965, *op. cit.*; également : A.-L. Mie, *op. cit.*, pp. 157 et 158.

[22] Cf. notamment, J. Baud, *op. cit.*, p. 103.

UEO a fait l'objet d'une instruction interministérielle n° 2101 du SGDN du 1er décembre 1975 (non publiée) [23].

Mais, suite à l'entrée en vigueur du nouveau Code pénal, qui a créé un lien juridique entre la protection pénale et l'existence de mesures de classification administratives (cf. supra), le gouvernement s'est vu obligé de renforcer l'assise réglementaire de ces classifications interalliées. Ce fut l'objet de l'arrêté du Premier ministre en date du 25 février 1994 [24]. Celui-ci établit purement et simplement l'assimilation aux niveaux de classification français des mentions équivalentes de l'OTAN, de l'UEO et de l'EURATOM (qui possède également ses trois niveaux : *Très secret Atomal*, *Secret Atomal*, *Confidential Atomal*, *Atomal Restricted*). Par cet artifice juridique, l'administration française fait en sorte qu'un document classifié d'une de ces organisations internationales soit automatiquement considéré comme faisant partie des secrets de défense tels que protégés par les articles 413-9 et suivants du Code pénal.

À l'inverse, en ce qui concerne les classifications nationales utilisées dans chacun des États alliés (qu'il est donc impossible de considérer comme directement intégrés dans les secrets de défense français), seules des dispositions législatives peuvent aujourd'hui permettre de leur assurer une protection pénale équivalente sur le territoire français [25]. Cette protection accordée aux secrets alliés trouvait, jusqu'en 1994, son fondement dans les articles 103 et R. 24 du Code pénal [26]. Désormais, elle est assurée au travers de l'article 414-8 du nouveau Code pénal qui dispose que

> *« Les dispositions des articles 411-1 à 411-11 et 413-1 à 413-12 sont applicables aux actes visés par ces dispositions qui seraient commis au préjudice des puissances signataires du traité de l'Atlantique Nord. »* [27]

Cet article est suivi d'un article spécifique concernant la Suède. En effet, ayant constaté que le seul pays non-membre de l'OTAN avec lequel la France avait passé un accord de sécurité (et donc auquel elle avait étendu sa protection au titre du dernier alinéa de l'article R. 24) était

---

[23] Mentionnée – ainsi que son homologue sur l'OTAN dans le *Guide sur la sécurité de défense dans les programmes d'armement (nationaux et avec l'étranger)*, n° 140/DEF/CAB/BS du 24 novembre 1994, p. 8.

[24] Arrêté du 25 février 1994 relatif à la détermination du niveau de classification de certains secrets de la défense nationale, *JORF*, 1er mars 1994, p. 3328.

[25] Après la déclaration de guerre de 1939, le gouvernement – usant de ses pouvoirs spéciaux – avait pu, par un simple décret du 26 septembre 1939, étendre aux actes commis à l'encontre des pays alliés (Grande-Bretagne et Empire britannique, Canada, Australie, Nouvelle-Zélande, Afrique du Sud, Pologne) les dispositions pénales françaises réprimant les atteintes contre la sûreté extérieure de l'État.

[26] L'article 103 ouvrait au Gouvernement le droit d'étendre, par décret en conseil des ministres, le bénéfice *« des dispositions relatives aux crimes et délits contre la sûreté de l'État aux actes concernant celle-ci qui seraient commis contre les États de la Communauté ou contre les puissances alliées ou amies de la France »* et l'article R. 24 pris par décret en application de l'article 103 prévoyait, justement, cette extension au profit des *« puissances signataires du traité de l'Atlantique Nord »* (art. R. 24.2°).

[27] On remarque, à cette occasion, que le système de délégation réglementaire pour l'extension aux pays étrangers a été abandonné, car comme le signale la circulaire de la Chancellerie, elle revenait *« à donner à l'autorité réglementaire le pouvoir d'étendre, et donc de créer, des crimes et des délits : seul le législateur est compétent pour procéder à de telles extensions »* (Ministère de la Justice, Circulaire du 14 mai 1993 présentant les dispositions du nouveau Code pénal et de la loi n° 92-1336 relative à son entrée en vigueur, *JORF*, octobre 1993, p. 234).

la Suède [28], le législateur a donc créé également l'article 414-9 qui étend législativement les dispositions pénales au bénéfice du Royaume de Suède.

La disparition récente de l'ancienne mention « diffusion restreinte »

En deçà des classifications de secret, la France comme la plupart des autres pays occidentaux et l'OTAN, possédait une mention de niveau inférieur qui visait simplement à empêcher la communication au public de documents ou d'informations qui, sans être secrets (ni même pouvoir mener directement à des secrets, comme c'est le cas pour les informations classifiées *Confidentiel-Défense*) doivent demeurer couverts par les règles du secret professionnel ou de ce que l'on appelle dans l'administration, la *« discrétion professionnelle »* (cf. infra). Les autorités françaises utilisaient pour ce faire la mention *« Diffusion Restreinte »* dont le décret du 12 mai 1981 disait simplement, dans son article 6 qu'*« il appartient à chaque ministre d'organiser suivant les nécessités de son département la protection des informations qui doivent faire l'objet d'une diffusion restreinte »*.

L'usage de cette mention provoquait deux effets juridiques complémentaires : d'une part, la communication d'un document *« Diffusion Restreinte »* à une personne non autorisée entraînait l'application des dispositions pénales sur le secret professionnel et la discrétion professionnelle ; d'autre part, elle contribuait à rendre le document non communicable au public (la CADA avait, par exemple, décidé de refuser l'accès à l'instruction interministérielle n° 1300 sur la protection du secret, pour cause de *« Diffusion restreinte »* [29]), ainsi que cela résultait indirectement des orientations fixées aux ministères par le SGDN :

> *« D'une manière générale, toutes les informations d'un Département ministériel qui ne sont couvertes ni par le secret de défense, ni par une mention de protection de confidentialité spécifique, mais qui sont considérées comme non communicables au public, doivent recevoir la mention Diffusion Restreinte. »* [30]

Mais dans le nouveau contexte créé par la révision du Code pénal, le statut et les effets juridiques de la mention *Diffusion Restreinte* étaient devenus plus ambigus. En effet, une lecture littérale des dispositions de l'article 413-9 pouvait conduire une juridiction à présumer que toute violation des restrictions de communication liées à cette mention était susceptible de constituer un atteinte au secret de défense, puisque la nouvelle définition pénale crée une présomption de secret de défense pour toute information *« intéressant la défense nationale qui ont fait l'objet de mesures de protection destinées à restreindre leur diffusion »*, ce qui peut s'appliquer – du fait de la généralité de la formule – à toutes les informations *« Diffusion Restreinte »* relatives à la défense nationale.

Outre que cette perspective aurait eu pour conséquence de faire prolifération les cas de poursuites pénales, elle aurait contredit, par ses

---

[28] Cf. l'accord de sécurité franco-suédois du 22 octobre 1973, publié au *JORF.* par le décret n° 76-469 du 28 mai 1976.

[29] Cf. infra, Chapitre 9 et l'avis *Syndicat CFDT des métallurgistes du Nord de la Seine*, 24 octobre 1985.

[30] *Protection des informations sensibles ne relevant pas du secret de défense - Recommandations pour les postes de travail informatiques*, n° 600/SGDN/DISSI/SCSSI, janvier 1990, p. 4.

possibles conséquences (à savoir, une condamnation pour violation du secret de défense), le principe même du *« Diffusion Restreinte »*, qui était d'être une mention de discrétion qui échappait au dispositif pénal de protection du secret de défense. Dans ces conditions et suivant des avis juridiques exprimés en ce sens [31], l'autorité réglementaire a choisi de supprimer ce niveau de classification qui n'est plus mentionné dans le décret du 17 juillet 1998.

Les classifications internes à certains organismes

Au même niveau que l'ancienne mention *Diffusion Restreinte*, il faut relever l'existence de certaines classifications internes à des organismes publics ou para-publics. Les mesures de protection des informations mises en place par ces organismes s'apparentent, pour l'essentiel, à de simples mesures d'ordre privé visant à assurer la protection du secret de fabrique ou de secrets d'affaires, mais lorsque ces organismes publics travaillent dans des domaines sensibles et que les informations en question sont traitées par des personnels de statut public (soumis de ce fait à des obligations de discrétion professionnelle particulières), ces classifications s'assimilent finalement à une extension et une survivance de la mention *« Diffusion restreinte »*, voire peuvent entraîner l'application de mesures de protection du niveau *Confidentiel-Défense*, sans en avoir pour autant le statut juridique [32]. Il existe, par exemple, des mentions *« Confidentiel-industrie »*, *« Confidentiel-technologie »*, ou encore *« Confidentiel-commercial »*.

Mais le cas le plus important en cette matière concerne le Commissariat à l'Energie Atomique (CEA) au sein duquel il existe des procédures internes de protection du secret très rigoureuses, mais qui ne relèvent du système classique de protection du secret de défense qu'en partie (celle qui concerne directement les activités de la Direction des Applications militaires du CEA [33]).

Pour le reste, le *« Secret CEA »* appartient à cette zone floue des classifications parallèles, comme l'a reconnu officiellement le Gouvernement en réponse à la question d'un parlementaire en 1982 :

> *« La notion d'information de défense nationale est prise dans son acception la plus large en raison du caractère d'universalité de la défense affirmée par l'ordonnance du 7 janvier 1959* (...) *Lorsqu'il s'agit*

---

[31] Cf. notamment, notre position dans notre thèse, Bertrand Warusfel, *Le secret de la défense nationale - Protection des intérêts de la nation et libertés publiques dans une société d'information*, thèse, Université Paris V, 1994, p. 210.

[32] *« Ces mentions ne sont pas des classifications. Elles indiquent que l'information, qui ne concerne jamais la défense nationale, doit cependant être protégée avec le plus grand soin, et notamment qu'elle ne doit jamais être communiquée à des personnes non autorisées par l'autorité hiérarchique. Bien que les règles de protection prescrites par ce guide ne s'appliquent pas aux informations Confidentiel + qualificatif, il est recommandé de s'inspirer des règles concernant le Confidentiel défense, afin de garantir la meilleure protection possible. »* (*Guide pratique sur la protection du secret de défense*, SGDN, édition 1990, p. 3).

[33] La presse a fait état, lors de l'arrrestation en 1992 de F. Temperville de documents internes à la DAM classifiés « Vulcain », ce qui constituerait une classification *Très Secret-Défense* spéciale relative aux armes nucléaires françaises (cf. *Le Point*, 24 octobre 1992, p. 48; *Le Figaro*, 24-25 octobre 1992).

d'informations ne relevant pas du secret de défense nationale, il faut distinguer celles qui sont traitées par des établissements ou des entreprises publiques de celles qui concernent des entreprises privées. Le premier cas intéresse essentiellement le commissariat à l'énergie atomique. S'inspirant des textes réglementaires précités, ce dernier a créé un « secret CEA » (dont les règles générales sont élaborées par une commission spéciale) et un « secret Cogema » qui couvrent toutes les informations considérées comme sensibles au plan de l'innovation industrielle et du patrimoine du groupe CEA. » [34]

Pour autant, la pratique du CEA est de traiter la protection de l'ensemble des secrets qu'il possède (qu'ils soient ou non des secrets liés à la défense) grâce à un système uniforme de classification, auquel l'on accède au travers d'une procédure d'habilitation spécifique géré directement par le CEA et son service de sécurité [35]. Si, dans la pratique, ce *« Secret CEA »* autonome fait penser aux *« Restricted Data »* américaines qui couvrent toutes les informations secrètes relatives au nucléaire civil et militaire, il existe cependant de grandes différences juridiques entre ces deux systèmes : aux Etats-Unis, en effet, ce dispositif de classification spécifique pour le nucléaire résulte d'une loi particulière, l'*Atomic Energy Act* de 1946 qui comporte ses propres sanctions pénales, lesquelles en font la catégorie de secrets de défense la mieux protégée des Etats-Unis [36]. En France, en revanche, nous ne connaissons aucune disposition réglementaire spécifique au secret dans le domaine des technologies nucléaires, à la seule exception – très spécifique et très limitée – du décret du 3 avril 1980 qui instaure un contrôle préalable sur les études et recherches *« dans le domaine de la fusion thermonucléaire par confinement inertiel »* [37].

Les compétences administratives en matière de classification

La responsabilité de la protection des secrets de la défense nationale est essentiellement confiée aux ministres, même si les décisions de classification sont prises par les chefs de service.

---

[34] *JORF Débats Assemblée nationale*, 1er mars 1982, réponse à la question écrite n° 7338 du 28 décembre 1981.

[35] Pierre Péan mentionne notamment la volonté affirmée d'André Giraud, administrateur général du CEA de 1970 à 1976, qui réforma le système du secret au sein du CEA et pratiqua volontairement une politique *« d'autonomie du système de protection »*, allant jusqu'à se méfier aussi bien des autorités gouvernementales, que des militaires ou même de la DST (P. Péan, *op. cit.*, pp. 99 à 102).

[36] Cf. par exemple, James R. Newman, « Control of Information Relating to Atomic Energy », *The Yale Law Journal*, Vol. 56, mai 1947, n° 5, pp. 769 et s.

[37] Décret n° 80-247 du 3 avril 1980 relatif aux activités d'études et de recherches dans le domaine de la fusion thermonucléaire par confinement inertiel, *JORF*, 6 avril 1980. Ce décret prévoit que *« toute personne physique ou morale se disposant à entreprendre ou à faire entreprendre des études et recherches dans le domaine de la fusion thermonucléaire par confinement inertiel doit en faire la déclaration auprès du secrétariat général de la défense nationale »*. Un comité spécialisé donne un avis sur le projet ainsi que sur son exécution et les éventuelles publications ou communications, en vue de respecter le secret de défense. Les travaux sur financement public dans ce domaine doivent faire l'objet d'une autorisation explicite du Premier ministre. Ce système – institué dans un domaine critique pour le développement des armes nucléaires de nouvelle génération et de la simulation des explosions nucléaires – est le seul système français prévoyant un contrôle préalable sur des recherches ou publications scientifiques (alors qu'aux Etats-Unis, par exemple, certains aspects de la cryptographie font l'objet de dispositions similaires). Cf. Michel

Le rôle des ministres

En dehors du ministre de la Défense (cf. infra) et du ministre de l'Intérieur, dont dépend la DST, aucun ministre ne possède directement de fonction opérationnelle directe en matière de contre-espionnage. Cependant, ils participent indirectement à l'activité de contre-espionnage préventif. En effet, en tant que responsables des responsabilités de défense relevant de leur département (en vertu de l'article 15 de l'ordonnance du 7 janvier 1959), ils définissent chacun les directives internes relatives à la protection des informations classifiées jusqu'au niveau *Secret-Défense* (le *Très Secret-Défense* étant protégé et géré directement par le Premier ministre, c'est-à-dire le SGDN).

Cette compétence ministérielle est, en réalité, exercée de manière permanente, par le Haut fonctionnaire de défense de chaque département ministériel qui *« est responsable de l'application des dispositions relatives à la sécurité de défense et à la protection du secret »* [38].

Dans les ministères qui possèdent des services ou des organismes sous tutelle particulièrement concernés par la protection du secret, le Haut fonctionnaire de défense peut se faire assister de différents *« fonctionnaires de sécurité de défense »* [39], dont l'un aura plus particulièrement en charge les questions liées à la sécurité informatique.

Une des manifestations de la compétence ministérielle en matière de détermination du secret dans leur département a été la publication par les principaux ministères des arrêtés prévus dans le cadre des textes organisant l'accès aux documents administratifs (cf. infra, chapitre 9). Ces textes fixent, notamment, dans chaque ministère les contours du périmètre du secret de la défense nationale. Mais pour autant, ces textes n'ont pas pour fonction de limiter le pouvoir du ministre de classifier éventuellement d'autres types d'informations, qui appartient à tout chef de service.

En deçà du secret de défense, chaque ministre est également responsable de la protection des informations non communicables au public, dont la confidentialité relève de la *« discrétion professionnelle »* et qui faisait l'objet, jusqu'au décret de juillet 1998, de la mention *Diffusion Restreinte.*

La situation particulière du ministère de la Défense

L'article 16 de l'ordonnance de 1959 confie au ministre de la défense la responsabilité de veiller à la sécurité des forces armées et des services qui en dépendent. Il ne dispose donc pas d'un Haut fonctionnaire de défense, mais dispose – nous l'avons vu – d'un service de sécurité dédié à cette mission ministérielle de sécurité des forces et de protection du secret, la DPSD [40].

Ferrier, « La non-prolifération : une question d'actualité », *Relations internationales*, n° 69, printemps 1992, p. 67.

[38] Article 2 du décret n° 80-243 du 3 avril 1980 relatif aux attributions des hauts fonctionnaires de défense.

[39] Cf. Henri Debrun, « Le secret de défense » in Jacques Robert (sous la dir.) *L'esprit de défense*, Economica, 1987, p. 447.

[40] Bien qu'abritant aussi des services impliqués dans le contre-espionnage (DST et RG) le ministère de l'Intérieur ne dispose pas de son propre service interne. Cela n'empêche pas la DST

Au niveau du cabinet du ministre, un conseiller technique est simplement désigné comme fonctionnaire de sécurité et de défense. De même, à chaque échelon du commandement, un officier est désigné comme officier de sécurité et gère, à ce titre, les relations avec la DPSD. À la Délégation générale pour l'Armement (DGA), il existe – outre des officiers de sécurité aux différents niveaux de la hiérarchie – un bureau central de sécurité qui dépend directement du cabinet du Délégué général.

La responsabilité des chefs de service dans la décision de classification

Quel que soit le département ministériel concerné, si la responsabilité de fixer les règles du secret appartient au ministre, la décision de classifier une information (c'est-à-dire de choisir pour cette information la mise en œuvre des mesures de protection liées à son niveau de sensibilité) revient au chef de service, responsable de l'organisation de son service. Cela amène dans la pratique à une déconcentration très importante du pouvoir de classification [41].

Mais cette déconcentration n'empêche pas l'application des règles normales de l'action administrative et du pouvoir hiérarchique (qui donne notamment le pouvoir de réformation à l'autorité administrative supérieure). Et, de plus, le ministre peut toujours, dans le cadre des directives qu'il adresse à ses services en matière de protection du secret, limiter à certaines autorités limitativement définies le droit de classifier certaines catégories d'information ou de recourir à certains niveaux de protection.

On doit signaler cependant que jusqu'à aujourd'hui, le statut juridique précis des décisions de classification des informations et documents confidentiels n'a pas été clairement établi par la jurisprudence administrative. Tout au plus peut-on considérer que la tendance actuelle (notamment depuis l'entrée en vigueur du nouveau Code pénal) conduit naturellement à reconnaître à ces décisions (tout comme aux décisions d'habilitation) le caractère d'actes administratifs susceptibles d'être soumis au contrôle du juge administratif.

La gestion et la protection des informations classifiées

Chaque niveau de classification se distingue des autres, non seulement par ses critères de définition (cf. supra) mais surtout par les mesures de protection qui y sont liées.

---

d'enquêter, le cas échéant, sur d'autres fonctionnaires de la police nationale : ce fut le cas, il y a une quinzaine d'années, lorsqu'un haut fonctionnaire de la Préfecture de police de Paris fut fortement soupçonné de travailler pour les services tchécoslovaques (cf. Th. Wolton, *Le KGB en France*, Grasset, 1986, pp. 63 à 67); plus récemment, en 1986 la DST a interrogé et fait muter un inspecteur des RG (cf. Jean Guisnel & Bernard Violet, *Services secrets - le pouvoir et les services de renseignement sous François Mitterrand*, La Découverte, 1988, pp. 97 à 103).

[41] À titre de référence, on peut estimer qu'aux États-Unis, bien qu'il n'y a actuellement que 5.400 chefs de services habilités (par un écrit du Président) à prendre des décisions de classification, 3 millions de fonctionnaires gouvernementaux ou d'employés d'entreprises sous contrat possèdent – par délégation – un tel pouvoir (chiffres cités dans le rapport de la Commission Moynihan : *Report of the Commission on Protecting and Reducing Government Secrecy*, Senate Document 105-2 pursuant to public Law 236, 103rd Congress, US GPO, Washington, 1997).

C'est, ainsi, par exemple, qu'il faut bien comprendre qu'entre le *Secret-Défense* et le *Très Secret-Défense* qui sont deux mentions qui couvrent des secrets de défense au sens strict, la véritable différence pratique n'est pas dans la teneur de l'obligation de secret, mais dans le renforcement des mesures de protection applicables et des peines encourues.

Sans entrer dans tous les détails de ces procédures qui précisent avec minutie les règles applicables à la gestion pratique des supports d'informations classifiées – et qui sont, elles-mêmes souvent confidentielles – nous indiquerons simplement les principes essentiels qui les gouvernent.

Il s'agit, pour l'essentiel, de règles concernant l'identification, la diffusion et la conservation de ces supports.

L'identification des supports

L'identification des supports d'information classifiée se fait, chaque fois que cela est possible, par le marquage de ce support d'une manière normalisée indiquant le niveau de classification et rappelant à toute personne amenée à voir ce marquage que l'accès à ce support est réservé à des personnes spécialement qualifiées pour ce faire [42]. Ce marquage remplit, en effet, une double fonction :

– une fonction administrative, qui permet aux détenteurs qualifiés de connaître le niveau de classification du document de manière à lui permettre de respecter les mesures de sécurité appropriées ;

– une fonction juridique, qui met en connaissance de cause les détenteurs qualifiés aussi bien que les tiers du caractère confidentiel du document, ce qui devrait permettre ultérieurement de présumer le caractère intentionnel d'une éventuelle compromission de ce secret.

Mais si le marquage est la solution d'identification appropriée à la protection d'informations sous forme imprimée, cette technique devient plus délicate à employer dans le cas d'objets (machines, dispositifs, armes, maquettes, ...), voire inadaptée à la protection des informations sur support immatériel (exposés oraux, stockage et transmission d'informations sous forme électronique). C'est là l'une des difficultés pratiques auxquelles les méthodes traditionnelles de protection du secret sont confrontées du fait de l'évolution des techniques et des modes de travail.

La diffusion des supports

La diffusion des supports d'information classifiée est le second aspect essentiel de cette méthodologie de protection et de gestion des supports

---

[42] Certains auteurs ont relevé le caractère paradoxal du marquage du secret : « *Notons ce paradoxe d'un secret qui se matérialise, qui prend forme, qui se montre. Le plus sûr des secrets n'est-il pas celui qui s'est libéré des marques qui le dénoncent, partant, qui a pris les apparences de la plus grande publicité ? Le secret politique contemporain, bureaucratisé, paperassier, fier de lui-même, récuse la logique de la dissimulation qui a inspiré « La Lettre volée » : il a besoin de se faire reconnaître. Cette ambition de reconnaissance a elle-même des effets. Pour l'habilité, qui se voit à chaque feuillet reconnaître qu'il appartient au monde de ceux qui savent. Pour l'espion à l'affût du tampon révélateur. Pour l'outsider, porté à donner valeur à ce dont il est exclu* » (A. Dewerpe, *op. cit.*, pp. 141 à 142).

du secret. Le principe en est la limitation de la diffusion aux personnes qualifiées et, pour ce faire, l'organisation d'une « traçabilité » permanente des supports. Les règles en question – plus ou moins strictes suivant les niveaux de classification [43] – interviennent à un double niveau :

– le tirage et la reproduction des documents ne peuvent être assurés que dans des conditions permettant à l'autorité émettrice de garder un contrôle sur ces opérations et de permettre l'enregistrement et la numérotation des exemplaires réalisés [44]. De plus, la réglementation distingue entre les reproductions partielles et totales, lorsqu'il s'agit de documents *Secret-Défense* [45]. Ces règles sont généralement complétées par des mesures propres à chaque type de moyen de reproduction (photocopieuse, télécopieur, imprimante, micrographie...) ;

– la circulation physique des supports est encadrée par des obligations portant, notamment sur l'établissement de listes de diffusion, l'enregistrement des personnes en ayant reçu communication, l'envoi du courrier sous double enveloppe et les bordereaux d'accompagnement [46], l'utilisation de convoyeurs ayant reçu un agrément particulier.

La conservation et la destruction des supports

La conservation des supports d'informations classifiées est le dernier aspect sensible de la gestion des supports qui fait l'objet de règles contraignantes pour les détenteurs d'informations classifiées. Il faut savoir qu'il s'agit d'un problème fort important étant donné le volume fréquemment élevé d'informations classifiées détenues par certains services. À titre d'exemple, on a pu évaluer le nombre de documents annuellement classifiés aux USA à 6,8 millions de documents en 1989, à 6,3 millions

---

[43] Sur le plan des principes, la grande distinction existant entre les règles de diffusion des informations classifiées « *Confidentiel-Défense* » et celles classifiées « *Secret-Défense* » est que le « *Confidentiel-Défense* » « *nécessite une surveillance régulière* » alors que le « *Secret-Défense* » « *exige une surveillance permanente* » (Georges Herrmann, *Guide pour la sécurité industrielle - guide à l'usage des agents de sécurité responsables de la protection du secret dans les marchés classés de défense nationale*, chez l'auteur, mars 1984, p. 31).

[44] À titre d'exemple des risques que peut comporter une gestion non rigoureuse des règles régissant la reproduction et la diffusion des documents classifiés : des plans de matériel classifié (lance-roquette) ainsi que ceux de plusieurs administrations (sous-sol du siège de la Banque de France) et entreprises, retrouvés dans les poubelles d'une société spécialisée en reproduction de documents techniques (*Minute*, 8 décembre 1984, p. 18); des plans d'une centrale nucléaire espagnole trouvés en pleine rue à Paris (*Le Canard enchaîné*, 11 septembre 1985); des courriers et des télex relatifs à une négociation sur la vente de sous-marins reçus par erreur par une agence de voyage (*Le Canard enchaîné*, 6 août 1986). Plus sérieusement, Wladimar Zolotarenko, employé subalterne au service reprographie de l'AGARD – agence de l'OTAN installée en France – fut condamné en février 1984 pour avoir photocopié au profit du KGB de nombreux documents classifiés (cf. André Giresse & Philippe Bernert, *Seule la vérité blesse – L'honneur de déplaire*, Plon, 1987, réédition : Presses Pocket, 1988, p. 325; Th. Wolton, *op. cit.*, pp. 148 et 149). Et cette pratique paraît ancienne : en 1912, l'Amirauté britannique se serait procuré le projet de loi sur le renforcement de la marine allemande grâce un agent qui subtilisa un jeu d'épreuves dans l'établissement chargé de l'impression des documents du Reichstag (cf. Hector C. Bywater & H.C. Ferraby, *Intelligence Service - Souvenir du service secret de l'Amirauté britannique*, édition française : Payot, 1932, p. 89).

[45] Cf. P. Péan, *op. cit.*, pp. 50 à 52; Guide SGDN, *op. cit.*, p. 24.

[46] Cf. P. Péan, *op. cit.*, pp. 57 et 58; Guide SGDN, *op. cit.*, pp. 18-23.

en 1992 [47] et à 3,6 millions en 1995 (dont 400.000 au niveau *Top Secret*) [48]. Et il resterait encore dans les archives américaines, plus d'un milliard et demi de pages classifiées ayant plus de 25 ans d'âge [49].

Pour l'essentiel, les contraintes ont trait aux sites de stockage et d'utilisation des supports concernés : si le *Confidentiel-Défense* ne requiert que la conservation des documents dans des armoires fortes, les classifications supérieures obligent à la création d'une *« zone réservée »*, voire d'une *« zone protégée »* dont les accès sont contrôlés et qui sont placés sous surveillance.

Mais la destruction des supports classifiés est aussi soumise à des règles précises dont le but est d'éviter qu'à l'occasion d'une destruction incomplète ou fictive, une information secrète puisse être compromise sans que l'organisation de sécurité détecte cette fuite. Les règles de destruction portent sur l'utilisation de techniques appropriées, sur la nécessité de garder trace de la destruction (sur cahier d'enregistrement ou par procès-verbal suivant les cas) et sur les personnes et autorités habilitées à effectuer cette opération ou devant être prévenues de celle-ci (dans certains cas, l'autorité d'origine).

L'archivage et la déclassification des informations classifiées

Lorsqu'une information classifiée a cessé d'être directement utile ou exploitable, se pose pour son détenteur la question de son devenir. Nous avons vu précédemment que la réglementation prévoyait la possibilité de destruction du support sous certaines conditions, mais de nombreuses raisons peuvent amener le détenteur à souhaiter ou devoir conserver le support d'information concerné. Se pose, dans ce cas, un double problème : celui de son archivage et celui de son éventuelle déclassification.

L'archivage des informations classifiées

Si la compatibilité des mesures de protection du secret avec les obligations légales en matière d'archives publiques (dont les textes sont en cours de réforme) est étudiée plus loin, il nous faut, pour autant, rappeler déjà ici les règles pratiques qui sont observées actuellement pour l'archivage des documents classifiés :

– l'archivage des documents *« Très Secret-Défense »* est impossible, les services d'archives n'étant au mieux qu'habilités à recevoir des documents classifiés du niveau *« Secret-Défense »*. Leur archivage ne peut donc survenir qu'après une décision éventuelle de déclassification (cf. infra) ;

– les documents classifiés doivent faire l'objet, dans les mêmes conditions que toutes les archives publiques, d'un tri avant archivage en vue

---

[47] Pour 1989, chiffres cités par l'*International Herald Tribune* du 19 avril 1990; pour 1992, chiffres tirés du rapport de l'Information Security Oversight Office (*AFP*, 8 mars 1993; A. & H. Toffler, *op. cit.*, p. 225).

[48] Ces derniers chiffres – qui témoignent d'une tendance forte à la décroissance des décisions de classification depuis plusieurs années aux USA – sont cités dans le rapport de la Commission Moynihan (*Report of the Commission on Protecting and Reducing Government Secrecy*, Senate Document 105-2 pursuant to public Law 236, 103rd Congress, US GPO, Washington, 1997).

[49] Rapport Moynihan, *op. cit.*

de « *séparer les documents à conserver et les documents dépourvus d'intérêt administratif et historique, destinés à l'élimination* » (article 4 de la loi sur les archives) ;

– seuls trois services d'archives sont habilités pour conserver des documents classifiés de niveau « *Confidentiel-Défense* » ou « *Secret-Défense* ». Il s'agit du service historique des armées (pour le ministère de la défense), des archives du ministère des affaires étrangères (pour les archives diplomatiques) et de la direction des Archives nationales (pour l'ensemble des autres administrations et organismes civils) ;

– conformément à l'article 7.5° de la loi sur les archives et de l'article 6 du décret relatif aux archives de la défense, les documents classifiés « *Secret-Défense* » et « *Très-secret* » ne peuvent être librement consultés qu'après un délai de soixante ans [50]. Pour les documents « *Confidentiel-Défense* », s'applique, en revanche, le délai de droit commun de trente ans (article 6.4° de la loi sur les archives), sauf lorsque ces documents appartiennent, par leur contenu, à certaines des autres catégories définies par le décret sur les archives de défense comme relevant du délai de soixante ans [51]. L'un des axes de la réforme actuellement à l'étude devrait concerner la réduction de ces délais (cf. infra, chapitre 9).

Mais toutes les informations classifiées ne nécessitent que leur classification survive à leur versement aux archives. Au contraire, certaines d'entre elles peuvent faire l'objet d'une décision de déclassification.

La déclassification

La déclassification est une procédure prévue par les textes organisant la protection du secret. Elle peut être plus ou moins poussée : soit la déclassification complète qui fait perdre au document tout caractère secret et le rend potentiellement communicable, soit l'abaissement de classification, qui permet d'alléger les mesures de protection à exercer et d'accroître le nombre des personnes qualifiées pouvant potentiellement en prendre connaissance (c'est, notamment le cas lorsqu'un document classé « *Secret* » devient simplement « *Confidentiel* », ce qui signifie – en principe – que l'information en elle-même n'a plus de caractère secret, mais que la lecture du document pourrait néanmoins donner des indications à un adversaire potentiel sur la manière d'accéder à d'autres secrets).

Cette déclassification est une décision qui peut être prise, outre pour des raisons de réduction des coûts liés à la protection, pour adapter cette protection à l'évolution dans le temps de la valeur de l'information

---

[50] Le fait que les documents « *Très Secret-Défense* » ne soient communicables qu'après soixante ans n'est pas contradictoire avec le fait que ces documents ne peuvent être versés aux services d'archives. En effet, le décret sur les archives de défense considère comme « *archives courantes* » les documents qui demeurent entre les mains des services qui les ont produits ou reçus, catégorie dans laquelle rentrent les documents « *Très secret-Défense* ».

[51] Ce sont « *les dossiers, rapports et fiches de renseignement à caractère nominatif mettant en cause la vie privée ou intéressant la sûreté de l'État ou la défense nationale; les dossiers des deuxièmes bureaux des états-majors et des bureaux de renseignement et de relations internationales militaires; les dossiers du SDECE; les archives des services de gendarmerie mettant en cause la vie privée ou intéressant la sûreté de l'État ou la défense nationale; les dossiers de la sécurité militaire* » (Décret n° 79-1035, art. 6).

protégée. Le temps est, en effet, l'une des variables essentielles de la « sensibilité » d'une information confidentielle :

> *« Pour les documents intéressant la défense, le secret est susceptible d'évoluer et même de disparaître avant l'expiration de ce délai* [des 60 ans de non-consultation des archives – cf. infra]. *Par exemple, le secret qui entoure, de manière extrêmement stricte, des opérations militaires, perd souvent de sa sensibilité dès la fin de celles-ci : il en est ainsi pour les patrouilles de sous-marins nucléaires, dont le retour est tenu secret jusqu'au moment où le SNLE a regagné sa base. »* [52]

Après avoir ignoré longtemps (jusque dans les années soixante [53]) cette nécessité de la déclassification, la réglementation française donne la possibilité (même si cela ne paraît pas être une pratique totalement entrée dans les mœurs) à l'autorité émettrice de prévoir, à l'avance, un terme à l'issue duquel la classification initiale sera réduite ou supprimée automatiquement. Et l'instruction n° 1300 proposait, à titre indicatif, le délai de 10 ans pour le *« Secret-Défense »* et de 5 ans pour le *« Confidentiel-Défense »* [54].

Aux Etats-Unis, cette pratique de la déclassification périodique a toujours été au cœur des débats engagés sur le contrôle des services de renseignement et les risques d'*« overclassification »* [55] (sur ce sujet, cf. infra). Après que l'Executive Order n° 10501 du président Eisenhower eut fixé en 1953 une limite de durée de classification de douze ans pour les documents *Top Secret* (avec certaines exceptions), l'Executive Order n° 11652 (du président Nixon en 1972) puis l'Executive Order n° 12065 (du président Carter en 1978) organisèrent chacun des procédures de déclassification automatique au bout d'une certaine période pour chaque niveau de classification. Mais ce système de déclassification automatique fut abrogé par l'Executive Order n° 12356 signé par le président Reagan le 2 avril 1982, qui se contentait de prévoir en remplacement des procédures de révision des classifications, soit de manière automatique par les services d'archives, soit même à la demande d'un citoyen américain ou de n'importe quelle institution américaine [56]. Avec la publication du nouvel Executive Order n° 12598 du président Clinton, il est à nouveau prévu une déclassification de principe au bout de 10 années, mais assortie d'un certain nombre d'exceptions permettant le maintien au secret de certains documents particulièrement sensible [57].

La déclassification peut aussi, plus rarement, être décidée en fonction du contexte et de la situation environnante. C'est fréquemment le cas aux États-Unis, au travers de l'utilisation par les médias et les citoyens du Freedom of Information Act (FOIA) qui leur permet de requérir de

---

[52] H. Debrun, *op. cit.*, p. 444.

[53] Cf. Jean Planchais, « Les charmes du secret », *Le Monde*, 5 janvier 1984.

[54] Cité par P. Péan, *op. cit.*, p. 49.

[55] Cf. sur ce sujet Repr. William S. Moorhead, « Operation and Reform of the Classification System in the United States » *in* Thomas M. Franck & Edward Weisband (ed.), *Secrecy and Foreign Policy*, Oxford University Press, 1974, pp. 87 et s.

[56] *National Security Information*, Executive Order 12356 du 2 avril 1982, 47 F.R. 14874, *US Code Congressionnal and Administrative News* – 97th Congress Second Session, 1982, n° 4, Section 3.3.(a)(b), pp. B57 à B58.

[57] Sur l'historique des différents réglements présidentiels, cf. le rapport Moynihan, *op. cit.*

l'administration américaine l'accès (et donc – le cas échéant – la déclassification) à toute information détenue par celle-ci.

C'est parfois aussi le cas au cours de procédures judiciaires dans lesquelles les magistrats demandent à l'autorité administrative la déclassification d'une information pour les besoins de leur instruction [58]. Comme nous le verrons d'ailleurs, la récente loi du 8 juillet 1998 créant une Commission consultative du secret de la défense nationale a institué une procédure spécifique permettant aux juridictions désireuses de se voir communiquer une information classifiée de demander formellement à l'administration la déclassification de cette information.

Mais quels que soient le motif et l'initiative de la demande de déclassification, le principe général en droit administratif français du *« parallélisme des formes »* s'applique, bien évidemment, en la matière. C'est l'autorité émettrice (et *in fine*, le Premier ministre, chef de l'administration) qui a seule la possibilité de modifier et d'assouplir le niveau de classification initiale, ainsi que le prévoit l'article 4, alinéa 2 du décret du 17 juillet 1998 : *« Les modifications ou les suppressions des mentions sont décidées par les autorités qui ont procédé à la classification. »*

L'HABILITATION DES PERSONNES

Une fois l'information et son support classifiés, la procédure de protection du secret s'intéresse aux détenteurs potentiels de ce secret. Or, contrairement à l'adage populaire selon lequel *« secret de trois : secret de tous »*, le nombre des personnes habilitées est très important dans les pays industrialisés. À titre d'exemple, les statistiques américaines dénombraient en 1986 près de 3 millions et demi de personnes habilités [59]. Parmi celles-ci, environ 500.000 personnes étaient habilités *Top Secret* [60]. De plus, près de la moitié des Américains habilités travailleraient dans l'industrie répartis au titre des contrats de recherche ou d'armements [61]. On ne dispose pas de tels chiffres pour la France, mais des sources journalistiques avancent le nombre de 8.000 habilités au sein du seul CEA [62], et estiment à plusieurs milliers le nombre d'enquêtes d'habilitation effectuées chaque année par la DPSD [63]. Il s'agit donc bien, en France également, d'une gestion de masse qui requiert des règles très précises.

Le contrôle des personnes ayant accès au secret va reposer sur un système à double niveau : la procédure d'habilitation, dont nous étudierons successivement les objectifs et les modalités, puis l'appréciation du *« besoin*

---

[58] On l'a vu en France dans plusieurs affaires contemporaines, comme dans l'« affaire Luchaire » ou celles des « Avions renifleurs », du « Carrefour du développement » ou encore des « écoutes téléphoniques de l'Élysée », affaires dans lesquelles la demande de déclassification a été diversement accueillie par les autorités gouvernementales (cf. infra, chapitres 10 et 11).

[59] Chiffre cité par l'*International Herald Tribune*, 30 mai 1986.

[60] Chiffre de 1986 extrait du *Federal Government's Security Clearance Program*, 1986, cité par Chapman Pincher, *Traitors – The Labyrinths of Treason*, Sidgwick & Jackson, Londres, 1987 – réédition 1989, p. 176.

[61] « Pentagon to Overhaul Policies on Secrecy Procedures », *Defense News*, 14/20 septembre 1992, p. 6.

[62] Cf. le dossier spécial « La force de frappe tranquille », *Canard Enchaîné*, n° 12, septembre 1984, p. 54.

[63] J. Guisnel & B. Violet, *op. cit.*, p. 125.

d'en connaître ». Mais le rappel et l'engagement éventuel de la responsabilité de la personne habilitée reste l'outil dissuasif le plus efficace pour assurer la sécurité des informations classifiées.

Les objectifs de la procédure d'habilitation

La sécurité du secret repose sur le fait que n'auront accès à lui que des personnes ayant été préalablement sélectionnées, en fonction de leur aptitude à respecter les règles de sécurité liés à la classification. Ce premier préalable à l'accès à l'information classifiée (le second étant le « *besoin d'en connaître* » – cf. infra) constitue la procédure d'habilitation (appelée dans les pays anglo-saxons, le système du « *positive vetting* » [64]).

L'obligation de recourir à cette procédure a été précisée réglementairement pour la première fois par les articles 7 et 8 du décret du 12 mai 1981. Avant cette date – mis à part les personnels militaires pour lesquels la procédure d'enquête préalable à tout engagement se fondait déjà sur l'article 88 du statut général des militaires [65] – la pratique des habilitations ne faisait l'objet d'aucun fondement législatif ou réglementaire publié. Elle n'était régie – comme les autres dispositions administratives de protection du secret – que par des instructions internes et non publiées, et ne reposait qu'*a contrario*, et indirectement, sur le fait que le Code pénal a toujours connu la notion de « *personne non qualifiée* » pour connaître des secrets, ce qui laissait entendre qu'il existait des personnes qualifiées et donc, *a fortiori*, habilitées [66].

L'article 7 du décret du 17 juillet 1998 prévoit notamment que « *nul n'est qualifié pour connaître des informations ou supports protégés s'il n'a fait au préalable l'objet d'une décision d'habilitation et s'il n'a besoin de les connaître pour l'accomplissement de sa fonction ou de sa mission* ».

Mais son article 8 précise que cette décision d'habilitation « *précise le niveau de classification des informations ou supports protégés dont le titulaire peut connaître* » et « *intervient à la suite d'une procédure d'habilitation définie par le Premier ministre* ».

Cette disposition réglementaire décrit ainsi, de manière succincte, l'objet de l'habilitation : s'assurer, avant toute communication d'informations classifiées à une personne que celle-ci ne constitue pas un « *facteur de risques* » pour la sécurité des informations concernées. Les spécialistes de la protection du secret estiment, en effet, traditionnellement que l'être humain est souvent le « *maillon faible* » d'une organisation de sécurité et que ce qu'ils appellent la « *source humaine* » [67] demeure un canal très

---

[64] Cf. pour la Grande-Bretagne, Chapman Pincher, *Too Secret, Too Long – The great bretrayal of Britain's crucial secrets and the cover-up*, Sidwick & Jackson, Londres, 1984, p. 201 ; « Report of the Security Commission May 1985 », *HMSO*, Londres, Cmnd. 9514, pp. 22 à 24.

[65] « *Nul ne peut souscrire un engagement : (...) s'il ne présente les aptitudes exigées pour l'exercice de la fonction* » (article 88 de la loi n° 72-662 du 13 juillet 1972 portant statut général des militaires, *JORF*, 14 juin 1972, p. 7430).

[66] Il ne faut pas, pour autant, confondre personne « *qualifiée* » et personne « *habilitée* » (cf. infra, nos développements sur le « *besoin d'en connaître* »).

[67] En anglais : « *Human Intelligence* » (HUMINT), par opposition aux sources techniques : communications (COMINT), signaux (SIGINT), émissions électroniques (ELINT).

efficace pour connaître certaines informations confidentielles [68]. Or, comme le fait remarquer un spécialiste britannique, ayant longuement travaillé sur les cas de trahison survenus au Royaume-Uni depuis la seconde Guerre mondiale

> *« il y a un facteur commun dans l'équation de la trahison de la plupart des traîtres du temps de paix, c'est l'accès aux secrets. Les histoires connues en la matière indiquent qu'à chaque fois qu'un traître a décidé de transmettre de l'information, il a tendance à fournir tout ce qui lui tombe sous la main, sans discernement, utilisant comme matériau ce qui s'offre le plus aisément à lui. De ce fait, l'étendue des dommages infligés par un traître dépend de la qualité de l'accès dont il dispose et du temps durant lequel il va opérer. »* [69]

En termes administratifs, l'enquête d'habilitation qui va être effectuée concernant la personne à habiliter va tenter d'évaluer si celle-ci ne possède pas, du fait de tel ou tel aspect de sa vie (famille, activité, contacts, ... – cf. infra) une *« vulnérabilité particulière »* (ce sont les termes employés par le ministre de la défense dans plusieurs cas de refus d'habilitation soumis à l'appréciation des tribunaux, cf. infra), c'est-à-dire une faiblesse qui pourrait être exploitable par un service ou une puissance désireuse d'accéder à des informations secrètes [70].

La doctrine administrative (ainsi que l'article 8 de l'ancien décret de 1981) met sur le même plan que les intérêts de la défense nationale, la sécurité propre de la personne faisant l'objet de la procédure d'habilitation. En effet, faire accéder une personne « vulnérable » à des informations classifiées comporterait non seulement un danger pour la sécurité de ces informations, mais aussi pour la sécurité de cette personne qui risquerait d'être confrontée à des tentatives d'exploitation de ses vulnérabilités par

---

[68] Si les sources techniques concurrencent de plus en plus actuellement la source humaine pour de nombreuses fonctions (notamment en ce qui concerne le renseignement militaire opérationnel), l'utilisation de personnes physiques comme source d'information demeure indispensable pour certaines tâches : connaissance de l'état d'esprit et du contexte dans lesquels évoluent les décideurs, assistance à certaines réunions, capacité d'influence sur certaines décisions (pour un écho de ce débat interne à la doctrine du renseignement, cf. A. Dewerpe, *op. cit.*, p. 251). C'est logiquement l'opinion du colonel Paillole pour qui *« l'homme demeure la ressource fondamentale de la recherche »* (préface au tome 1[er] de Roger Faligot & Rémi Kauffer, *Histoire mondiale du renseignement*, Robert Laffont, 1993, p. 7) ou encore de l'amiral Lacoste selon lequel *« on accorde beaucoup moins d'attention au facteur humain, alors qu'il est, à mon sens, le plus important de tous »* (P. Lacoste, *op. cit.*, p. 41). Plus surprenant, le futurologue américain Alvin Tofler n'hésite pas à affirmer que, par rapport à la *« Deuxième Vague »* du renseignement que nous avons connue jusqu'à maintenant (et qui se caractérisait par l'usage massif de moyens techniques) *« le passage à un système de renseignement de la Troisième Vague signifie, paradoxalement que l'on va donner plus d'importance aux espions humains : les seuls qu'avaient connus le monde de la Première Vague »* (A. & H. Toffler, *Guerre et contre-guerre – Survivre à l'aube du XXI[e] siècle*, Fayard, 1994, p. 224).

[69] Chapman Pincher, *op. cit.*, p. 174.

[70] Les milieux du renseignement résument souvent les principales causes de « vulnérabilité » amenant au recrutement par un service étranger, sous la forme de l'acronyme MICE (*« Monnaie, Idéologie, Chantage, Ego »*, cf. Th. Wolton, *op. cit.*, p. 134), ou de sa version anglo-saxonne, MISE (*« Money, Ideology, Sex, Ego »*, Constantin Melnik, *Un espion dans le siècle – La diagonale du double*, Plon, 1994, p. 222). L'un des reproches fréquemment formulés à l'encontre de la procédure d'habilitation tient à l'interprétation subjective et tendancieuse qui peut être faite de la notion de « vulnérabilité » : *« on sait combien cette notion (de vulnérabilité) est floue; ainsi le fait d'être homosexuel est considéré comme parfaitement dangereux par la SM, tout comme le fait de jouer aux courses : là encore les investigations s'étendent à la vie privée »* (Jean Dolent & Thomas Daquin, *La sécurité militaire*, Éditions du Cerf, 1981, p. 75).

une puissance tierce cherchant à faire pression sur elle pour qu'elle accepte de violer à son profit les règles de sécurité. En cas de refus d'habilitation, les autorités gouvernementales prennent d'ailleurs parfois le soin de faire comprendre que ce refus respecte les droits et les intérêts de la personne concernée :

> *« De telles mesures de protection et de prévention – tant à l'égard des personnes que des informations – n'affectent en rien l'honorabilité des agents. »* [71]

Mais bien que cet aspect des choses soit moralement indiscutable, on doit constater cependant que cette invocation de la sécurité personnelle de l'intéressé comme motif d'un possible refus d'habilitation demeure avant tout une manière élégante pour les autorités gouvernementales de faire accepter cette procédure et ses éventuelles conséquences par les citoyens qui en font l'objet.

Les modalités de la procédure d'habilitation

La procédure d'habilitation concerne en premier lieu les personnes physiques devant être amenées, de par leurs activités, à prendre connaissance et à traiter des informations secrètes. Mais elle peut également, dans certains cas, déboucher sur l'habilitation de personnes morales de droit privé, lorsque l'administration confie, par contrat, à un organisme privé cocontractant le soin de réaliser pour son compte des opérations comportant l'accès à de telles informations (cf. infra, nos développements sur la protection en milieu industriel).

La procédure d'habilitation des personnes physiques

La procédure d'habilitation des personnes physiques est engagée sur la base d'une demande formulée par l'autorité qui emploie la personne concernée ou qui veut lui confier l'exécution d'une tâche impliquant l'accès à des informations classifiées. Chaque demande d'habilitation se réfère à un degré de classification particulier *(Confidentiel-Défense, Secret-Défense, Très Secret-Défense)*. En matière de *Très secret Défense*, seul le Secrétariat général de la défense nationale a compétence pour faire instruire le dossier par les services spécialisés et pour prendre la décision d'admission (cf. supra).

La personne, objet de la procédure, remplit un formulaire de renseignements détaillé. Ce formulaire, dénommé *« notice individuelle »* comporte plusieurs rubriques portant notamment sur l'état civil, la famille [72], les activités professionnelles, les domiciles successifs et les voyages à l'étranger de la personne à habiliter [73]. De plus, cette

---

[71] *Assemblée nationale*, réponse à la question écrite n° 32165 du 2 novembre 1987, 14 décembre 1987, *JORF*, p. 6779.

[72] Outre la connaissance des ascendants et collatéraux de la personne concernée (dont les éventuelles origines étrangères ou la résidence hors du territoire national peuvent être l'occasion d'exercer des pressions), le conjoint éventuel fait l'objet de l'attention des services enquêteurs. Il en est particulièrement ainsi lorsqu'une personne ayant déjà accès à des informations classifiées épouse un conjoint ressortissant d'un pays étranger considéré comme *« sensible »* (cf. *Le Figaro*, 21/22 mars 1987).

[73] J. Dolent & T. Daquin, *op. cit.*, pp. 75 et 76; J. Guisnel et B. Violet, *op. cit.*, p. 125.

« notice individuelle que chaque candidat doit remplir en application de l'instruction générale interministérielle n° 1300/SGDN/SSD du 12 mars 1982, comprend trois rubriques portant sur la nationalité : nationalité à la naissance ; nationalité actuelle ; en cas de double nationalité, le préciser. Ces rubriques sont alimentées par la personne concernée qui s'engage sur leur exactitude par une mention signée à la fin du document. » [74]

Ce dossier est alors transmis à un service de sécurité et de contre-espionnage chargé d'effectuer une enquête à partir des renseignements fournis, d'identifier éventuellement et d'évaluer les vulnérabilités de la personne concernée et de faire connaître son avis technique au service demandeur [75].

Le plus important de ces services est la Direction de la protection et de la sécurité de la défense (DPSD) qui a repris, parmi les attributions traditionnelles de l'ancienne Sécurité militaire, celle d'effectuer des enquêtes d'habilitation [76], compétence qui a été spécifiquement consacrée par l'article 3 de son décret de création. L'une des divisions opérationnelles de sa direction centrale en est spécialement chargée [77]. Sa compétence en matière d'enquêtes d'habilitation couvre l'ensemble des personnels civils et militaires du ministère de la défense ainsi que celles relatives aux cocontractants de ce même ministère.

La Direction de la surveillance du territoire (DST) effectue, quant à elle, au titre de sa mission générale de sécurité et de protection du secret [78], les mêmes enquêtes d'habilitation en ce qui concerne les personnes ne relevant pas du ministère de la défense. Par ailleurs, les services des Renseignements généraux – bien que n'ayant de responsabilité directe dans les questions de protection du secret – sont généralement consultés par la DPSD ou la DST pour effectuer une partie des enquêtes relatives à ces demandes d'habilitation [79].

---

[74] *Assemblée nationale*, réponse à la question écrite n° 28718 du 27 juillet 1987, 7 septembre 1987, *JORF*, p. 5088.

[75] Une partie essentielle de l'enquête consiste à interroger les fichiers des différents services de police et de gendarmerie à propos de la personne concernée et recouper les données fournies dans la notice individuelle avec les éléments d'information disponibles dans les dossiers et les fichiers officiels. On a plus d'informations sur la pratique des enquêtes en Grande-Bretagne ou aux États-Unis. Au Royaume-Uni, notamment, le travail à partir du questionnaire individuel et des fichiers de police, est complété par des entretiens avec l'intéressé (cf. par exemple, les quelques détails fournis sur la pratique du *« positive vetting »* dans le rapport établi après l'arrestation de Michael Bettaney, ancien officier du MI 5 inculpé en 1984 pour avoir tenté de faire passer au KGB des documents classifiés : « Report of the Security Commission May 1985 », *op. cit.*, pp. 22 à 24; cf. également Labour Party, *Freedom and the Security Services*, p. 13, qui précise que ces enquêtes et entretiens demandent beaucoup de personnel : 180 personnes, par exemple, pour les seules habilitations du ministère de la défense, à l'exclusion de celles relevant des forces armées, du MI 5 ou du Foreign Office, qui possèdent leurs propres équipes d'enquêteurs).

[76] Cf. notamment P. Péan, *op. cit.*, p. 92.; J. Dolent & T. Daquin, *op. cit.*, pp. 74 à 77.

[77] Cf. J. Guisnel et B. Violet, *op. cit.*, p. 122.

[78] Article 2, alinéa 3 du décret n° 82-1100 du 22 décembre 1982 fixant les attributions de la Direction de la surveillance du territoire, *JORF*, 26 décembre 1982.

[79] Cf. Jean-émile Vié, *Mémoires d'un directeur des renseignements généraux*, Albin Michel, 1988, pp. 85-86 et 116. Ce rôle des RG dans les procédures d'habilitation est aujourd'hui officiellement attesté par l'aliné 2° de l'article 3 du décret du 14 octobre 1991 sur les fichiers des RG qui vise les informations qui *« concernent des personnes ayant obtenu ou sollicitant une autorisation d'accès à des informations protégées en application du décret du 12 mai 1981 »* (Décret n° 91-1051 du 14 octobre 1991 portant application aux fichiers informatisés, manuels ou

Mais en ce qui concerne les habilitations au *« Secret CEA »* (cf. supra), l'enquête préalable est confiée à sa direction de la sécurité (l'ancien DSPS), conformément aux règles très dérogatoires qui, comme nous l'avons vu précédemment, assurent une très large autonomie au CEA dans la conduite de sa sécurité (même si celui-ci fait également appel aux services des RG pour compléter ses propres enquêtes).

Une fois l'enquête effectuée, l'autorité demanderesse de l'habilitation reçoit communication d'un *« avis de sécurité »* [80] résumant les conclusions du service enquêteur [qui peuvent être de trois ordres : *« sans objection »*, *« défavorable »* ou *« restrictif »* [81]] et prend ou refuse [82] – sous sa propre responsabilité – la décision d'admission ou d'agrément [83] aux informations classifiées du niveau correspondant, sachant que *« l'accès au niveau le plus élevé permet l'accès aux niveaux inférieurs »* [84].

Cette décision n'est pas communiquée en tant que telle à l'intéressé auquel est seulement demandé de signer une attestation de reconnaissance de responsabilité (cf. infra).

Dès lors que la procédure d'habilitation s'est conclue sur une décision d'admission aux informations classifiées, le service demandeur dont dépend la personne habilitée effectue une gestion administrative (souvent informatisée) de ces dossiers d'autorisations d'accès au secret [85]. Pour leur part, les services de contre-espionnage ayant effectué l'enquête conservent les documents et les informations nominatives ayant été recueillies lors de cette enquête.

---

mécanographiques gérés par les services des renseignements généraux des dispositions de l'article 31, alinéa 3, de la loi n° 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, *JORF* du 15 octobre 1991, p. 13498).

[80] *« La DPSD délivre à l'attention du commandement des avis pour l'habilitation des personnes aux différentes catégories de secret »* (*Terre Information*, n° 171, février 1989, p. 6). Sur les restrictions d'accès à ces avis, cf. infra, chapitre 9.

[81] Cf. J. Dolent & T. Daquin, *op. cit.*, p. 76.

[82] Concernant le ratio entre décisions favorables et défavorables, le ministre de l'équipement a, par exemple, répondu en 1987 à une question parlementaire que *« les avis défavorables émis par les services spécialisés après instruction de demandes d'habilitations demeurent exceptionnels : de l'ordre de 2 à 3 % des demandes présentées. La réglementation susvisée exclut expressément la communication à qui que ce soit de leurs conclusions »* (*Assemblée nationale*, réponse à la question n° 32954 du 16 novembre 1987, *JORF*, p. 6985).

[83] À la différence de la décision d'admission qui est destinée à des personnes devant prendre connaissance de manière régulière d'informations classifiées, l'agrément de sécurité est accordé, à l'issue de l'enquête d'habilitation, à certaines personne qui n'auront qu'une *« connaissance fortuite et/ou occasionnelle d'informations « Secret défense » ou « Confidentiel défense » (...) : membres des conseils d'administration, cadres et employés de certains services commerciaux, certains convoyeurs, gardiens, personnels d'entretien, cabinets conseils, audits, commissaires aux comptes, ... »* (G. Herrmann, *op. cit.*, p. 55).

[84] R. Blaser, *op. cit.*, p. 84.

[85] On peut citer, à titre d'exemple de cette gestion, la base de donnée informatique constituée par le bureau Sécurité de la DGA : *« Il est créé au bureau Sécurité de la Délégation générale pour l'armement (DGA) un traitement automatisé d'informations nominatives dont la finalité est la gestion des autorisations d'accès aux informations classées de la défense. Ce traitement concerne le personnel habilité travaillant dans les sociétés privées ou les établissements de la DGA titulaires de marchés classés ou à clause de sécurité »*. Sont enregistrées – pour chaque personne habilitée – les données nominatives suivantes : *« L'identité (nom, prénom, date et lieu de naissance, numéro de carte d'identité ou de passeport); l'activité professionnelle (dénomination de la société, adresse, téléphone, grade et fonction); l'habilitation (numéro et date de la décision d'habilitation, la nature de l'avis de sécurité) »* (arrêté du 26 novembre 1992 relatif à la mise en œuvre d'un traitement automatisé de gestion des autorisations d'accès aux informations classées de défense à la délégation générale pour l'armement, *JORF*, 18 décembre 1992, p. 17316).

Qu'il s'agisse de l'habilitation d'une personne physique ou morale, celle-ci n'a qu'une durée de vie limitée et nécessite son renouvellement périodique, dès lors que la personne concernée peut toujours justifier de son *« besoin d'en connaître »* (cf. ci-dessous) à la date d'expiration de sa précédente habilitation. Une habilitation au *Très Secret-Défense* doit être renouvelée au bout de trois années, contre cinq ans pour le niveau *Secret* et le niveau *Confidentiel*[86], mais doit également être renouvelée (avec rédaction d'un nouveau questionnaire) lors de chaque modification de la situation de l'intéressé (situation familiale, ou professionnelle)[87].

On relèvera, enfin, que dans un but d'allégement des procédures d'habilitation, il existe une *« dispense de la condition d'habilitation en faveur des fonctionnaires titulaires de l'Etat pour l'accès à la classification Confidentiel défense exclusivement. Ceux-ci ont accès de plein droit à ce niveau de classification sur la base du besoin d'en connaître. »*[88]

La procédure d'habilitation des personnes morales

La procédure d'habilitation des personnes morales est mise en œuvre à chaque fois qu'une personne morale de droit privé, non déjà habilitée, devient titulaire d'un marché public dit *« marché classé de défense »*, c'est-à-dire un marché passé avec une administration pour l'exécution duquel le cocontractant aura communication d'informations classifiées (cf. infra, chapitre 8).

L'appréciation du « besoin d'en connaître »

L'accès d'une personne à une information classifiée ne nécessite pas seulement que cette personne ait fait l'objet d'une enquête d'habilitation

---

[86] Cf. A.-L. Mie, *op. cit.*, p. 167 (néanmoins, l'habilitation au *Confidentiel-Défense* peut être renouvelée une fois par tacite reconduction, pour autant que la situation du titulaire n'ait pas été modifiée).

[87] Cf. G. Herrmann, *op. cit.*, pp. 55 et 56.

[88] R. Blaser, *op. cit.*, p. 84. A ce propos, il convient de signaler qu'une tradition ancienne veut que les ministres et leur entourage proche (leur cabinet, notamment) ne fassent pas l'objet de la procédure d'habilitation, alors même que leurs fonctions gouvernementales peuvent les amener à consulter et à créer des documents confidentiels (cf. l'ancien directeur du SDECE, qui le regrettait : Christine Ockrent & Alexandre de Marenches, *Dans le secret des princes*, Stock, 1986, p. 143). La raison doit en être trouvée dans la légitimité politique et démocratique qu'ils incarnent. C'est la raison qu'invoque, par exemple, le sénateur J. Thyraud lorsqu'il défend le droit d'accès aux informations classifiées pour les parlementaires tout en refusant l'idée même d'une habilitation : *« ses membres* (du Parlement) *ne sont soumis à aucune hiérarchie qui puisse les habiliter au Secret-Défense lorsqu'ils ont « besoin d'en connaître ». Ils tiennent de leur mandat et de la confiance de leur assemblée, la possibilité d'y avoir accès, dans le cadre des missions dont elle les charge »* (Proposition de loi tendant à remédier à l'usage abusif du Secret-Défense, présentée par M. Jacques Thyraud, *Sénat*, première session ordinaire de 1985-1986, séance du 15 octobre 1985, document n° 32, p. 7). Il faut savoir, à ce sujet, qu'en 1948, les membres de la Commission de la défense nationale de l'Assemblée ont voté une question préalable selon laquelle les secrets intéressant la Défense ne pourraient être évoqués en présence des députés communistes (cf. « Les secrets de la Défense nationale ne seront pas communiqués aux commissaires communistes » article paru dans *Le Figaro*, semaine du 30 octobre au 5 novembre 1948, reproduit in *Le Figaro-Magazine*, 5 novembre 1988, p. 191). Et en ce qui concerne les ministres, le problème s'est posé lors de la participation de ministres communistes au Gouvernement en 1981 : Marcel Chalet, alors directeur de la DST affirme que *« sans entrer dans des détails que je ne me sens pas autorisé à révéler, (qu')il a été fait, en sorte, au niveau gouvernemental, que, les principes étant saufs, les risques soient éludés »* (Marcel Chalet & Thierry Wolton, *Les visiteurs de l'ombre*, Grasset/Fasquelle, 1990, p. 291).

suivie d'une décision d'admission. Il faut également que pour chaque information classifiée, la personne habilitée justifie de son *« besoin d'en connaître pour l'accomplissement de sa fonction ou de sa mission »*, ainsi que le prévoit l'article 7 du décret du 12 mai 1981.

C'est là que réside la différence que nous avons évoquée plus haut entre une personne *« habilitée »* (c'est-à-dire ayant fait l'objet d'une décision d'admission positive) et la *« personne qualifiée »* auquel se réfère depuis longtemps le Code pénal pour caractériser les infractions à la protection du secret. Cela a été, d'ailleurs, confirmé lorsqu'au cours des débats parlementaires sur le projet de nouveau Code pénal, un amendement a proposé de remplacer dans l'article 413.10 l'expression *« personne non qualifiée »* par celle de *« personne non habilitée »*, ce que le Gouvernement a refusé en expliquant que

> *« le Gouvernement souhaite, sur ce point, que la formulation initiale, juridiquement plus exacte, soit conservée. Comme vous le savez, il ne suffit pas d'être habilité pour être qualifié ; cela ressort très clairement des textes organisant la protection des secrets de la défense nationale. »* [89]

Ce *« besoin d'en connaître »* est donc un élément essentiel pour l'accès à des informations classifiées et son appréciation fait partie des garanties que met en place l'organisation administrative de protection du secret de défense. Pour autant, les textes publiés – tout comme l'analyse de la pratique – ne permettent pas toujours de définir avec précision les modalités et le contenu exact de cette obligation. Tout au plus peut-on estimer que :

– la liberté d'accès aux informations classifiées n'est pas un droit acquis attaché à l'habilitation et à la décision d'admission ;

– le besoin d'en connaître paraît essentiellement lié à l'exercice d'une fonction ou d'une mission [90] ;

– la personne habilitée à un niveau donné de classification, pourra accéder, non pas à la totalité des informations classifiées de ce niveau, mais seulement à celles d'entre elles qui seront en rapport avec les missions précises qui lui seront confiées [en effet, *« faire dépendre ce besoin* (d'en connaître) *de la seule considération du poste occupé, en une sorte de facteur de prestige, constituerait un détournement de la règle de droit »* [91]] ;

– le changement de fonction ou la fin de la mission confiée à l'intéressé fait disparaître sa capacité d'accès aux informations classifiées, alors même que la durée de péremption de l'habilitation n'a pas encore été atteinte.

Si tous ces points paraissent indiscutables et indiscutés, il faut cependant relever que la situation est moins claire en ce qui concerne les modalités pratiques de détermination du besoin d'en connaître. Dans le silence des textes réglementaires sur le sujet, il nous paraît que ce besoin

---

[89] Intervention de M. Vauzelle, garde des sceaux, séance du jeudi 23 avril 1992, n° 25 S (CR), *JORF Sénat débats* du 24 avril 1992, p. 803).

[90] *« Selon l'interprétation administrative qui est faite de ce texte réglementaire, le « besoin d'en connaître » doit être entendu comme une obligation liée aux fonctions exercées et non comme un droit personnel à prendre connaissance de l'information. L'appréciation de ce besoin relève de l'autorité compétente pour l'habilitation »* (J. Thyraud, *Sénat*, document n° 32, *op. cit.*, p. 4).

[91] R. Blaser, *op. cit.*, p. 84.

s'apprécie en fonction de différents critères, tenant d'un côté à la volonté de l'autorité hiérarchique (qui peut avoir confié par écrit à son subordonné le soin d'accéder à telle information particulière, voire à une catégorie générique d'informations classifiées) et de l'autre, à l'analyse des fonctions et des activités exercées par la personne habilitée.

Cette appréciation paraît relativement aisée dans le cadre de marchés classés de défense puisque ceux-ci constituent, en eux-mêmes, la preuve du *« besoin d'en connaître »* de l'entreprise et, de plus, précisent dans leur annexe de sécurité les activités et les informations qui sont considérées comme classifiées. Elle l'est moins, en revanche, dans le cas d'une personne physique habilitée employée dans un service ou un organisme possédant certaines informations classifiées. Dès lors que la personne concernée ne peut pas produire un document de sa hiérarchie lui donnant, directement ou indirectement, mission de prendre connaissance de ces informations, le risque existe qu'en cas de litige (disciplinaire ou pénal), cette personne puisse se voir contester son besoin de connaître certaines informations et donc être considérée, *a posteriori*, comme étant, en l'espèce, une *« personne non qualifiée »* pour en prendre connaissance, avec toutes les conséquences que cela peut entraîner [92].

Les responsabilités des personnes habilitées

Les personnes habilitées et ayant à connaître des informations classifiées, assument, de ce fait, une obligation de confidentialité qui leur interdit de communiquer les supports d'information protégés auxquels ils accèdent à des personnes qui ne seraient, comme eux, qualifiées pour en connaître.

L'attestation de reconnaissance de responsabilité

Cette obligation est normalement matérialisée par l'attestation de reconnaissance de responsabilité que l'autorité hiérarchique fait signer par la personne concernée avant de donner accès aux informations classifiées. Dans cette attestation, la personne habilitée reconnaît avoir connaissance des dispositions pénales et réglementaires relatives à la protection du secret et des conséquences auxquelles elle s'exposerait dans le cas où elle laisserait communiquer ces informations à une personne non qualifiée. Une autre version de cette attestation doit, généralement, être signée par la même personne dans le cas où elle cesse les fonctions qui lui donnaient accès aux informations classifiées [93].

---

[92] L'arrêt du Conseil d'État *Demoiselle Faucheux* (cf. infra) – bien que ne traitant pas du besoin de connaître de documents classifiés, mais simplement de la communication (pour des motifs syndicaux) d'un document interne à une administration – montre, néanmoins, les limites strictes de la notion de personne ayant besoin de connaître d'une information. Il a sanctionné, en effet, un agent public, ayant pris connaissance d'un document dans le cadre de ses fonctions, pour avoir porté celui-ci à la connaissance de ses collègues, lesquels – bien qu'également agents de la même administration – devant être considérés comme des *« tiers »* au regard de l'obligation de discrétion professionnelle qui est imposée aux fonctionnaires de par la loi (CE, *Demoiselle Faucheux*, 6 mars 1953, note M. Waline, *RDP* 53, p. 1035).

[93] La pratique d'un engagement signé est également en vigueur aux États-Unis et en Grande-Bretagne mais, dans ces pays, elle revêt une beaucoup plus grande importance et sert de véritable engagement contractuel entre la personne habilitée et le Gouvernement (cf. notamment

L'analyse juridique de cette obligation amène à distinguer en elle deux niveaux complémentaires :

– une responsabilité pénale principale découlant de la violation des dispositions directement relatives au secret de défense ou aux intérêts fondamentaux de la nation ;

– une responsabilité disciplinaire complémentaire liée – pour les agents publics – à la violation des obligations générales de discrétion professionnelle et de réserve et – pour les salariés de droit privé – aux règles du droit du travail.

Si la responsabilité pénale découlant des dispositions du Code sur le secret de défense et les intérêts fondamentaux de la nation n'appelle d'autres commentaires que ceux déjà fournis précédemment lors de l'analyse de ces textes (cf. supra), il convient d'expliciter la responsabilité disciplinaire secondaire et de comprendre la manière dont elle peut se concilier avec la précédente.

La responsabilité disciplinaire des agents publics

Les fonctionnaires sont soumis aux dispositions du statut général de la fonction publique, qui prévoit, dans son article 26 (tel qu'il résulte de la loi du 13 juillet 1983 portant droits et obligations des fonctionnaires) :

> *« Les fonctionnaires sont tenus au secret professionnel dans le cadre des règles instituées par le Code pénal. Les fonctionnaires doivent faire preuve de discrétion professionnelle pour les faits, informations ou documents dont ils ont connaissance dans l'exercice ou à l'occasion de l'exercice de leurs fonctions. En dehors des cas expressément prévus par la réglementation en vigueur, notamment en matière de liberté d'accès aux documents administratifs, les fonctionnaires ne peuvent être déliés de cette obligation de discrétion professionnelle que par décision expresse de l'autorité dont ils dépendent. »*

Les militaires, pour leur part, sont soumis aux dispositions de l'article 18 du statut général des militaires :

> *« Indépendamment des dispositions du Code pénal relatives à la violation du secret de la défense nationale ou du secret professionnel, les militaires sont liés par l'obligation de discrétion pour tout ce qui concerne les faits et informations dont ils ont connaissance dans l'exercice ou à l'occasion de leurs fonctions. Tout détournement, toute communication contraire aux règlements, de pièces ou documents de service à des tiers est interdit. En dehors des cas expressément prévus par la réglementation en vigueur, les militaires ne peuvent être déliés de cette obligation de discrétion ou relevés de l'interdiction édictée à l'alinéa précédent qu'avec l'autorisation du ministre. »*

Relevons tout de suite, les deux différences qui distinguent ces textes, par ailleurs très proches dans leurs principes :

– D'une part, la loi de 1983 fait une place explicite aux règles sur la liberté d'accès aux documents administratifs, qu'elle considère comme

---

sur les poursuites engagées, aux Etats-Unis, à la suite du livre de Frank W. Snepp, ancien agent de la CIA : Diane F. Orentlicher, « *Snepp v. United States – The C.I.A. Secrecy Agreement and the First Amendment* », Columbia Law Review, Vol. 81.1, avril 1981, n° 3, pp. 662 et s.; Idem

une exception permanente (mais relative [94]) à la règle de la discrétion professionnelle, alors que le statut des militaires – antérieur à la loi de 1978 – ne parle que des cas *« expressément prévus par la législation en vigueur »*. Pour autant, il ne fait aucun doute que, comme l'indique la loi de 1983, les dispositions sur l'accès aux documents administratifs font partie des cas prévus par la réglementation en vigueur, et constituent donc également une exception à la discrétion professionnelle des militaires, dans les mêmes conditions que pour les autres fonctionnaires.

– D'autre part, la loi de 1983 ne parle que des dispositions pénales concernant le secret professionnel, alors que le statut des militaires évoque également les dispositions pénales relatives au secret de la défense nationale. Là encore – même s'il faut déplorer que la question n'ait pas été abordée explicitement [95] il ne faut tirer de cette omission aucune conséquence particulière : les dispositions du Livre IV du Code pénal s'imposent aux agents publics – qu'ils soient civils ou militaires – de la même façon qu'à tous les autres citoyens, et ne font que se surajouter à l'obligation de discrétion professionnelle qui est la leur. On peut même dire que les agents publics civils et militaires sont encore plus particulièrement visés que les autres citoyens par les dispositions de l'article 413-10 qui répriment la compromission du secret par son dépositaire, lequel est majoritairement un agent de l'État.

Du point de vue qui nous concerne, il convient d'éliminer d'emblée le secret professionnel prévu par le Code pénal (ancien article 378, nouveaux articles 226-13 et 226-14), et ce pour trois raisons. Premièrement, la jurisprudence constante en la matière réserve, en effet, l'application de cette notion à certaines catégories spécifiques de personnes privées (avocats, médecins, prêtres, ...) ou d'agents publics exerçant des fonctions particulières (officiers de police judiciaire contraints d'observer le secret de l'instruction, agents des P&T soumis au secret postal et des communications) à l'exclusion de tous les autres. Dès lors, l'ensemble des fonctionnaires ou militaires ne sont pas soumis au secret professionnel, au sens du Code pénal. Deuxièmement, il ne faut pas oublier la différence de nature qui existe entre le secret professionnel, qui est un secret personnel (c'est-à-dire attaché à une personne exerçant une certaine fonction, quel que soit le contenu des informations dont il prend connaissance à cette occasion) et le secret de défense qui est – peut-on dire – un *« secret réel »* attaché à certaines informations, quelle que soit la personne qui en prend connaissance [96]. Enfin – et surtout – la jurisprudence considère,

---

en Australie à l'encontre de Peter Wright suite à la publication de son livre *Spycatcher*, cf. chapitre 10).

[94] Le fait qu'un document soit communicable ne supprime pas l'obligation de discrétion professionnelle de l'agent public à son endroit. Il ne fait qu'empêcher celui-ci d'opposer l'obligation de discrétion à la personne qui a droit à cette communication (par exemple, le droit d'un étudiant à la communication de sa copie). Mais l'obligation continue à jouer à l'encontre des personnes qui n'ont pas le droit à communication de ce même document (cf. notamment, Jacques Robert (sous la dir.) *Étude de droit interne sur les notions de secret de défense et de patrimoine national et les règles de protection qui leur sont applicables*, non publiée, SGDN, janvier 1983, p. 13).

[95] Cette omission du secret de la défense nationale dans le texte de la loi de 1983 a été regrettée par un député lors des débats parlementaires (cf. intervention de M. Maurice Ligot, *Assemblée nationale, débats*, 2e séance du 4 mai 1983, *JORF*, p. 885).

[96] Sur cette distinction secret personnel/secret réel, cf. Françoise Gallouinec-Genuys & Herbert Maisl, *Le secret des fichiers*, IFSA/Editions Cujas, cahier n° 13, 1976. Pour une application de la

depuis la célèbre affaire *Arton* de 1896, que le secret professionnel institué par l'article 378 CP ne peut être invoqué qu'en faveur des particuliers et jamais pour protéger les intérêts publics que défend l'État [97].

Seule la loi sur les archives du 6 janvier 1979 (cf. infra, chapitre 9) a créé un cas particulier de secret professionnel permettant de sanctionner pénalement un agent public pour la divulgation d'un document confidentiel [98]. Ce secret professionnel s'impose à tous les agents affectés aux services d'archives et sa sanction pénale (et non seulement disciplinaire) peut se cumuler avec une infraction au secret de défense, dès lors que le document d'archives diffusé illégalement relève de cette catégorie de secret [99].

Dans les autres cas, la divulgation par un agent public [100] civil ou militaire d'une information confidentielle n'est punissable – du point de vue du droit de la fonction publique – que de sanctions disciplinaires, au titre de la violation des obligations de discrétion professionnelle ou de celle du *« devoir de réserve »* (imposées par l'art. 18 et l'art. 7 du statut des militaires, et dont la violation peut donner lieu à la révélation d'éléments couverts par la discrétion professionnelle, entraînant alors un cumul de fautes [101]). Tout au plus, dans certains cas, peut-il s'ajouter à cette responsabilité disciplinaire, la mise en cause de la responsabilité civile de l'agent [102] ou celle de la responsabilité de l'Administration [103].

La jurisprudence administrative a, par exemple, consacré l'application de ce pouvoir disciplinaire en cas de violation de la discrétion professionnelle dans l'arrêt *Noblet d'Anglure* [104], ou encore l'arrêt *Demoiselle Faucheux* déjà cité (sanction contre un responsable syndical diffusant au sein du service un document de travail).

---

notion de *« secret réel »* au secret de défense, cf. Bruno Lasserre, Noëlle Lenoir & Bernard Stirn, *La transparence administrative*, PUF, 1987, p. 10.

[97] T.C. Seine, 25 janvier 1896.

[98] *« Tout fonctionnaire ou agent chargé de la collecte ou de la conservation d'archives en application des dispositions de la présente loi est tenu au secret professionnel en ce qui concerne tout document qui ne peut être légalement mis à la disposition du public »* (article 2 de la loi du 3 janvier 1979 sur les archives, *op. cit.*).

[99] Ce cumul serait également possible lorsqu'une information protégée par le secret de défense, l'est, parallèlement, par le secret professionnel (par exemple, un document classifié faisant état d'informations sur l'état médical d'une personne, ou une information classifiée confiée à un avocat dans le cadre d'un dossier dont il a la charge). De même, la loi du 16 juillet 1980 (cf. infra, nos développements à propos de la protection des secrets économiques, chapitre 8) sanctionne pénalement la livraison à l'étranger, de certaines informations, qui peuvent – par ailleurs – être classifiées.

[100] Dans le cas d'agents publics ne relevant pas du statut général des fonctionnaires, ce sont généralement des dispositions contractuelles spécifiques qui les obligent à se plier à une obligation de discrétion professionnelle (c'est le cas, par exemple, pour les agents du CEA).

[101] Ce fut le cas, par exemple, lors de la révocation en conseil de discipline de l'inspecteur de police Antoine Gaudino, pour *« manquement à l'obligation de réserve et à la discrétion professionnelle »* du fait de la publication de son ouvrage *« L'enquête impossible »* (consacré à l'affaire des *« fausses factures du Sud-Est »*) (Cf. le procès-verbal du conseil de discipline de la police nationale du 14 mars 1991, reproduit in Antoine Gaudino, *Le procès impossible*, Albin Michel, 1992, pp. 245 à 265). Cette décision fut annulée en appel par le Conseil d'État.

[102] Cf. notamment Tribunal des Conflits, *Gérard*, 11 décembre 1909.

[103] Cf. notamment C.E., *Fleur-Santucci*, 25 octobre 1935, Rec. 983 ; CE, *Sesmat*, 6 avril 1951, Rec. 175.

[104] C.E., *Noblet d'Anglure*, 24 mai 1935, Rec. 594.

À l'opposé, les salariés de droit privé habilités à accéder à des informations classifiées (généralement dans le cadre de l'exécution par leur entreprise d'un marché classé ou à clause de sécurité, cf. infra) ne relèvent pas des dispositions disciplinaires de la fonction publique. Les conséquences non pénales d'une éventuelle compromission d'informations classifiées par leurs soins, doivent donc être cherchées dans l'application des règles disciplinaires prévues par le Code du travail.

À ce titre, le salarié se rendant coupable d'un acte compromettant une information classifiée peut faire l'objet d'une mesure disciplinaire décidée par son employeur (conformément à l'article L. 122-41 du Code du travail), pouvant aller jusqu'au licenciement (article L. 122-14 du Code du travail). Les motifs de ce licenciement, qu'il appartiendra, le cas échéant, au juge d'apprécier, pourront, vraisemblablement, être trouvés suivant les cas :

– dans le préjudice que risque de subir l'entreprise du fait de cette compromission [105] : si celle-ci a eu lieu dans le cadre d'un marché classé, il est, notamment, fort probable que ce marché sera résilié unilatéralement aux torts de l'entreprise et que son habilitation lui sera retirée ;

– dans le caractère gravement fautif que constitue la compromission d'une information qui a été confiée au salarié pour l'exécution d'un travail dans des conditions de sécurité données et, en aucun cas, pour en permettre la divulgation ;

– dans la violation éventuelle d'une clause de discrétion professionnelle que l'employeur avait peut-être introduite dans le contrat de travail du salarié, ou – en l'absence d'une telle clause – dans la violation d'une obligation implicite de discrétion qui pèse sur certaines catégories de fonctions [106] ;

– dans l'impossibilité de poursuivre le contrat de travail du salarié, du fait du retrait (fort probable) de son habilitation par l'administration [107] ;

– ou, au minimum, dans la perte de confiance qui résultera du fait que le salarié a commis un acte répréhensible pénalement [108].

---

[105] Ainsi que nous l'évoquerons plus bas, plusieurs décisions de justice ont consacré, sous certaines conditions, la possibilité de licencier un salarié qui n'a pu obtenir l'habilitation nécessaire à l'exercice de ses fonctions au sein de l'entreprise (cf. infra). L'une d'entre elles précise plus généralement, dans ses attendus, que *« l'entreprise privée qui travaille pour la défense nationale et est obligée d'assurer strictement le secret des fabrications, doit veiller à ce que son personnel réponde exactement aux qualités que l'État estime indispensables pour des travaux de ce genre, toute négligence à cet égard pouvant engager la responsabilité morale et même pénale de ses directeurs si, à la suite de l'inexécution des instructions de l'autorité militaire, dont il ne lui appartient pas d'apprécier la légalité, le secret d'une fabrication n'avait pu être entièrement sauvegardé »* (Cour d'Appel de Paris, 21e ch., *Sarl Rubanox c. Cothier*, 27 juin 1963, *Dalloz*, 1964, p. 48).

[106] Cf. par exemple, note Bertrand Warusfel sous Cass. Soc., 8 février 1990 et CA Dijon, 11 février 1987, affaire *Pardon*, *Droit de l'informatique et des télécoms*, n° 91/3.

[107] Sur les conditions dans lesquels le refus ou le retrait d'habilitation peut donner lieu à licenciement, cf. infra nos développements sur la conciliation de la protection du secret avec les règles de droit du travail. Pour des jurisprudences confirmant la possibilité de rompre le contrat de travail lorsque le refus d'habilitation entraîne une *« impossibilité prouvée de fournir du travail »* au salarié : Cons. Prudh. Cherbourg, 14 novembre 1984, *Maheo c/ CMR*; Cons. Prudh. Cherbourg, 13 février 1985, *Deslandes c/ CMR* (nons publiés).

[108] On mentionnera, paradoxalement, que le simple fait pour une salariée d'une entreprise travaillant pour la défense nationale, d'avoir signalé – sans en avertir son employeur – à la

LES RÈGLES RELATIVES À LA PROTECTION DES SITES

Si les règles d'habilitation visent à protéger les supports d'information classifiés contre les menaces « internes » (c'est-à-dire la divulgation non autorisée par des personnes appartenant ou en relation à la structure gouvernementale émettrice), il convient aussi d'assurer la sécurité de ces supports vis-à-vis des menaces « externes », comme, par exemple, l'intrusion de personnes étrangères dans des lieux où ils sont entreposés. Cette protection physique et juridique de différents sites « sensibles » trouve ses moyens, d'une part, dans les dispositions générales qui protègent les installations qui intéressent la défense nationale et d'autre part, dans les règles qui instaurent des zones spécifiquement dédiées à la préservation du secret ou du patrimoine.

La protection générale des installations intéressant la défense nationale

Indépendamment des contraintes de la protection du secret, les autorités responsables de la défense nationale, à savoir le Premier ministre et le ministre de la défense (responsable de la sécurité des forces armées), ont adopté ou ont fait adopter des mesures de protection générale qui protègent l'accès aux principales installations intéressant la défense. Il s'agit, d'un côté, des sites militaires eux-mêmes et, de l'autre, des sites civils considérés comme *« sensibles »*, au regard des exigences de la défense civile ou économique.

La protection des établissements militaires

Les sites militaires font depuis très longtemps l'objet de mesures de protection, tant physiques que juridiques [109]. Déjà, la loi du 18 avril 1886 réprimait différents actes dirigés contre la sécurité des sites ou navires militaires. Les textes successifs continuèrent à incriminer spécifiquement les atteintes à l'intégrité des établissements militaires, de manière à éviter tant les actes de sabotage que les risques de violation des secrets de défense. On citera, par exemple, l'article 82 issu de la modification du Code pénal de 1939 et repris intégralement en 1960 dans l'article 79 [110].

DPSD l'existence de faits qu'elle considérait comme pouvant aussi être constitutifs d'espionnage, a été jugé comme constituant une faute grave justifiant son licenciement (Cour d'Appel de Paris, 18e ch., *Thomson Sintra c. Vie*, 1er février 1991, confirmé par Cass. Soc., 2 juillet 1992).

[109] D'après une étude de marché européenne, les armées françaises entretenaient, en 1989, *« 59 sites de haute sécurité, 335 bases principales, 555 hôpitaux, baraquements et autres constructions et 3200 petites bases »* et les dépenses totales de la France pour assurer la sécurité de ces sites militaires, s'élevaient à l'équivalent de 172 millions de dollars (cf. *Sécurité militaire et services associés en Europe de l'Ouest*, étude E1243, Frost & Sullivan Ltd., février 1990).

[110] Il punissait par ses alinéas 1° à 5° différents agissements proches de ceux déjà sanctionnés en 1886, mais modernisées en fonction des nouvelles possibilités techniques du moment (aviation, transmission radio, photographie). Concernant ce dernier aspect des photographies de zones militaires, les travaux parlementaires consacrés en 1922 à une tentative de réforme du Code pénal (qui n'aboutit pas) indiquaient que *« dans l'état actuel de la législation* (de 1886), *les tribunaux restent désarmés à l'égard des éditeurs et des vendeurs de photographies d'ouvrage de défense. Les autorités militaires et judiciaires en sont réduites à inviter officieusement les éditeurs et vendeurs à remettre leurs clichés et les épreuves qu'ils possèdent et à s'abstenir de prendre de semblables vues. Il semble impossible d'accepter comme licite le fait de faire commerce de photographies dont la divulgation est reconnue dangereuse pour la défense nationale, et alors que la loi punit ceux qui*

En la matière, le nouveau Code pénal a choisi une approche formellement plus sélective. Incriminant spécifiquement les différents agissements permettant de rechercher, de découvrir et de communiquer soit des secrets de la défense nationale (articles 413-10 à 413-12, cf. supra – I^re Partie, Chapitre I^er), soit des éléments dont la divulgation au profit d'une puissance étrangère porterait atteinte aux intérêts fondamentaux de la nation (articles 411-1 à 411-11, cf. supra – I^re Partie, Chapitre II), son Livre IV réprime séparément le simple fait de violer l'intégrité de certains sites intéressant la défense. C'est notamment le cas des établissements militaires qui sont désormais protégés par l'article 413-5 nCP (qui correspondait précédemment au 1° de l'article 79) aux termes duquel

> *« Le fait, sans autorisation des autorités compétentes, de s'introduire frauduleusement sur un terrain, dans une construction ou dans un engin ou appareil quelconque affecté à l'autorité militaire ou placé sous son contrôle est puni d'un an d'emprisonnement et de 100.000 F d'amende. »*

Mis à part le fait que les peines encourues ont été – dans le souci, déjà évoqué, de les rendre plus aisément applicables – très fortement abaissées par rapport au texte précédent (un an au lieu de dix à vingt ans), cet article ne comporte qu'une innovation formelle : l'expression *« affecté à l'autorité militaire ou placé sous son contrôle »*, qui couvre – comme le texte ancien – tout le domaine militaire [111], ainsi, sans doute, que les sites qui peuvent être mis temporairement à disposition des armées, en cas d'opérations militaires ou d'événements particuliers [112]. Pour le reste, comme l'ancien article 79, l'article 413-5 s'applique sans qu'il soit besoin de prouver quelque autre intention (espionnage, sabotage, ...) dès lors que deux conditions cumulatives sont réunies : introduction sans autorisation et caractère frauduleux. Cette double condition a paru *« presque redondante »* à certains lors des travaux parlementaires [113]. Pourtant, elle prend tout son sens, à la lumière du nouvel article R. 644-1 nCP, introduit dans la partie réglementaire du Code par le décret du 29 mars 1993 [114] qui abrogea, en même temps, le décret du 6 février

---

fournissent ces photographies. » (Rapport de M. Guillaume Poulle, sur le projet de loi tendant à réprimer les délits d'espionnage et les agissements de nature à favoriser l'espionnage, *JORF*, Sénat, Débats, 14 juin 1922). Le nouveau texte de 1939 ne résolut cependant pas complètement ce problème, puisqu'après la guerre, on relève à ce sujet - une anecdote révélatrice de la difficulté qu'il peut y avoir à distinguer un secret de défense d'un document public : la DST alertée par le SDECE à propos d'une commande de 1.500 cartes postales représentant des vues d'avion, identifia l'acheteur : l'attaché de l'air adjoint de l'ambassade soviétique. Elle fut alors chargée d'une commission rogatoire en vue de saisir chez tous les fabricants de cartes postales les clichés pouvant représenter des zones d'intérêt militaire (Cf. Pierre Levergeois, *J'ai choisi la DST - Souvenirs d'un inspecteur*, Flammarion, 1978, p. 108 et s.).

[111] Dans ce sens, *Rapport sur le projet de loi portant réforme des dispositions du Code pénal relatives à la répression des crimes et délits contre la Nation, l'Etat et la paix publique*, par M. François Colcombet, Tome I, *Assemblée nationale*, neuvième législature, séance du 26 septembre 1991, document n° 2244, p. 74.

[112] Cette expression rejoint, en cela, celle employée dans le règlement de discipline générale dans les armées qui organise notamment la protection du secret *« dans les enceintes et établissements militaires ou, en campagne, dans les cantonnements ou véhicules, ainsi qu'à bord des bâtiments de la marine et des aéronefs »* (Article 24 du règlement de discipline générale dans les armées, Décret n° 82-598 du 12 juillet 1982, cf. infra).

[113] Ce fut le cas du rapporteur de l'Assemblée, M. Colcombet, *op. cit.*, p. 75.

[114] Décret n° 93-726 du 29 mars 1993 portant réforme du Code pénal (deuxième partie : décrets en Conseil d'Etat) et modifiant certaines dispositions de droit pénal et de procédure pénale, *JORF*, 30 mars 1993, pp. 5559 et s.

1981 réglementant l'accès aux établissements militaires. Cet article prévoit, en effet, que

> *« Hors le cas prévu par l'article 413-5, le fait, sans autorisation des autorités compétentes, de pénétrer, séjourner ou circuler sur un terrain, dans une construction ou dans un engin ou appareil quelconque affecté à l'autorité militaire ou placé sous son contrôle est puni de l'amende prévue pour les contraventions de la 4e classe.*
>
> *L'interdiction d'accès aux terrains, constructions, engins ou appareils visés à l'alinéa précédent fait l'objet d'une signalisation particulière lorsque aucune marque distinctive ne signale qu'ils sont affectés à l'autorité militaire ou placés sous son contrôle. ».*

En clair, la pénétration sans autorisation dans un site militaire est constitutif d'un délit s'il est possible d'en établir le caractère frauduleux (par exemple, violence, effraction, fausse identité ou apparence, ...), soit d'une simple contravention de 4e classe si ce caractère frauduleux ne peut être établi [115]. De plus, il faut comprendre le second alinéa de l'article R. 644-1 comme faisant de l'existence d'une marque ou d'une signalisation distinctive une condition de son application. Il est logique, en effet, que la pénétration sans intention frauduleuse ne soit punissable qu'à partir du moment où son auteur avait connaissance du fait qu'il pénétrait dans un site interdit.

Pour pouvoir mettre en œuvre ces dispositions pénales, les forces armées doivent donc organiser sur le terrain une protection physique de leurs établissements et un contrôle de leurs accès. Tous les établissements militaires possèdent à la fois une clôture limitant les risques de pénétration clandestine et aux entrées du site, du personnel de surveillance gérant une procédure de contrôle des accès [116]. Ce travail de protection est généralement assuré dans les sites militaires par la conjonction de trois types d'intervenants :

– des personnels militaires appartenant à l'unité implantée sur le site ou à des unités spécialisées dans la protection (la marine possède 1.900 fusiliers marins pour la protection des bases navales et l'armée de l'air plus de 1.500 fusiliers commandos de l'air [117]) ;

– la gendarmerie, soit au travers d'unités spécialisées implantées à l'intérieur des établissements (1.000 gendarmes maritimes dans les bases navales, 1.200 gendarmes de l'air [118] sur les bases aériennes, 400 gendarmes de l'armement dans les établissements de la DGA [119], Garde républicaine

---

[115] On peut voir dans cet article R. 644-1 nCP *« un complément de protection contre les rôdeurs et les curieux, ainsi qu'une arme de dernier recours contre des personnes soupçonnées de s'être introduites sciemment sur le site sans qu'il soit possible d'en apporter la preuve »* (Bertrand Warusfel, « Les zones protégées dans le nouveau Code pénal », *Droit et Défense*, n° 93/2, p. 61).

[116] À titre de court résumé du contenu de ces procédures, on peut se reporter à un arrêté d'août 1993 décrivant le contenu de la base de données type pour la gestion des accès (Arrêté du 23 août 1993 portant création d'un modèle type de traitement automatisé d'informations nominatives ayant pour objet le contrôle et la gestion des accès des établissements militaires, *JORF*, 9 septembre 1993, p. 12645).

[117] Cf. le dossier spécial sur la protection, *in Armées d'aujourd'hui*, n° 116, décembre 1986/ janvier 1987, p. 31 (la protection des bases navales) et p. 33 (la protection des bases aériennes).

[118] *Ibid.*

[119] Dans les établissements de l'armement, les gendarmes travaillent en parallèle avec des sociétés de gardiennage privées, titulaires de marchés à clauses de sécurité (cf. infra) avec la

dans certains bâtiments gouvernementaux [120]), soit par les brigades territoriales qui assurent, à l'occasion de rondes périodiques, la surveillance extérieure des installations militaires [121] ;

– la DPSD, dont les postes, détachements et antennes implantés sur les principaux sites militaires et auprès de tous les échelons hiérarchiques (cf. supra), cherche à détecter les éventuels risques d'intrusion ou d'atteinte à la sécurité des installations (l'une de ses missions), assure l'inspection des sites et sert de conseil au commandement en matière de sécurité [122].

Si les tâches de police judiciaire nécessaires à mettre en œuvre en cas de commission d'infractions aux règles décrites ci-dessus, ne peuvent être effectuées que par les forces de gendarmerie (valablement habilitées par le procureur de la République du lieu), il demeure cependant vrai qu'en cas de flagrant délit, l'article 73 du Code de procédure pénale donne qualité à *« toute personne »* pour appréhender son auteur et le conduire devant l'officier de police judiciaire le plus proche. Appliqué aux règles régissant la protection et l'accès aux établissements militaires, cela implique que lorsqu'une intrusion *« frauduleuse »* (c'est-à-dire passible de l'application de l'article 413-5, et non du seul article R. 644-1 [123]) est détectée, toutes les forces impliquées dans la tâche de sécurité, c'est-à-dire

> *« le chef de poste, la sentinelle ou/et tout militaire peuvent appréhender un individu s'étant introduit frauduleusement ou sciemment dans un terrain militaire ou une zone protégée. On peut appréhender, mais sans usage des armes, mais on ne peut pas détenir.* (...) [On] *doit aussitôt en aviser l'officier de police judiciaire le plus proche dans le meilleur délai possible. »* [124]

Dans les établissements militaires nécessitant une protection particulière, peut être créée une zone ayant le statut de *« zone militaire sensible »* (ZMS), bénéficiant d'une sécurité renforcée et dont le statut se rattache à celui des *« zones protégées »*, mises en place pour la protection du secret et nous en étudierons plus loin les modalités.

Avant d'en finir avec ce sujet de l'accès aux établissements militaires, signalons – pour mémoire – que l'application sur le territoire français du

---

DGA (Cf. *Info-DGA*, n° 27, avril-mai 1990, p. 36; *Armées d'aujourd'hui*, n° 47, janvier/février 1980, p. 32).

[120] Les régiments de la Garde républicaine, unité spécialisée de la Gendarmerie nationale, assure la protection des principaux centres gouvernementaux (Palais de l'Élysée, Hôtel Matignon, les Assemblées, certains ministères sensibles – tels que les Affaires étrangères ou la Défense). Ils sont parfois soutenus et renforcés par des escadrons tournants de la gendarmerie mobile. A titre d'exemple, sur le rôle des gardes républicains dans la protection de Matignon ou de l'Élysée, cf. Thierry Pfister, *La vie quotidienne à Matignon au temps de l'Union de la gauche*, Hachette, 1985, pp. 93 à 97 et Charles Debbasch, *L'Élysée dévoilé*, Albin Michel, 1982, p. 67.

[121] Cf. « La gendarmerie et la sécurité des établissements militaires », *Armées d'aujourd'hui*, n° 116, *op. cit.*, pp. 35 et 36. Sur une critique de l'efficacité de cette protection *« périphérique »* par la gendarmerie territoriale de certains sites sensibles (en l'occurrence, les centrales nucléaires d'EDF), cf. *Le Canard Enchaîné*, 18 avril 1990.

[122] Cf. notamment, l'interview du général Armand Wautrin, alors, directeur de la DPSD, *in Armées d'aujourd'hui*, n° 79, avril 1983, pp. 6 et 7.

[123] On conçoit, cependant, que la distinction parfois subtile entre une simple intrusion *« sans autorisation »* et une intrusion réellement *« frauduleuse »* demeure difficile à faire, ce qui peut conduire, dans la pratique, à une interprétation extensive de la notion de *« flagrant délit »*.

[124] *Lettre d'information de l'Inspection de la Défense Opérationnelle du Territoire*, n° 2-93.

traité sur les forces armées conventionnelles en Europe [125], implique désormais que des *« inspections de défiance »* peuvent avoir lieu dans les établissements militaires (ainsi qu'éventuellement, dans des lieux dépendant de personnes privées ou de personnes publiques autres que l'État [126]).

Ajoutons, enfin, à tous ces éléments concernant l'accès aux établissements militaires qu'en leur sein, deux dispositions réglementaires spécifiques concernant la protection du secret à l'intérieur ou à proximité des sites militaires :

– l'article 24 du règlement de discipline générale dans les armées, qui impose à tous militaires certaines contraintes destinées à empêcher l'appropriation non autorisée d'informations pouvant être confidentielles [127] ;

– le nouvel article R. 645-2 du Code pénal, qui punit d'une contravention de la 5e classe un comportement, jusqu'alors réprimé d'une peine de dix à vingt ans de détention criminelle par l'article 79.4°, à savoir le fait d'effectuer des *« dessins, levés ou enregistrement d'image, de sons ou de signaux de toute nature »* dans une *« zone d'interdiction fixée par l'autorité militaire »*. Outre un très sensible allégement des peines encourues, cette nouvelle rédaction modernise la liste des activités interdites en visant les différentes formes d'enregistrement possibles, s'alignant ainsi sur les nouveaux moyens techniques d'espionnage (écoute électronique ou radioélectrique, surveillance vidéo, ...).

La protection des points sensibles

La France connaît une double structure de protection, la structure militaire et la structure de défense, qui englobe la structure militaire et lui adjoint d'autres éléments répondant notamment aux exigences de la défense civile et économique. Dans le cadre de cette organisation globale de la défense, a été élaborée la réglementation et la protection des *« points sensibles »*, définie par l'ordonnance du 29 décembre 1958 [128] et précisée par une instruction interministérielle récente [129].

---

[125] Cf. la loi n° 91-1399 du 31 décembre 1991 autorisant la ratification du traité sur les forces armées conventionnelles en Europe (ensemble huit protocoles), signé à Paris le 19 novembre 1990 (publié par le décret n° 93-183 du 2 février 1993) et la loi n° 93-893 du 6 juillet 1993 relative à la conduite des inspections menées en vertu de l'article 14 du traité sur les forces armées conventionnelles en Europe et du protocole sur l'inspection annexé à ce traité. Pour un premier commentaire de ces textes, cf. David Ruzié, « Actualités sur la participation de la France aux accords sur la sécurité collective », *Droit et Défense*, n° 93/2, p. 57.

[126] Cf. le décret n° 94-116 du 4 février 1994 pris pour l'application de la loi n° 93-893 du 6 juillet 1993, *JORF*, 11 février 1994, p. 2351.

[127] *« 1. La détention et l'usage d'appareils photographiques, cinématographiques ou enregistreurs ainsi que de postes émetteurs de radiodiffusion ou télévision dans les enceintes et établissements militaires ou, en campagne, dans les cantonnements ou véhicules, ainsi qu'à bord des bâtiments de la marine et des aéronefs, peuvent être soumis à autorisation préalable des chefs de corps et de service dans les conditions fixées par le commandement.*

2. La publication ou la cession de films, de photographies ou d'enregistrements pris dans les enceintes, établissements militaires, bâtiments de la marine et aéronefs ou à l'occasion d'opérations, de manœuvres ou de toute autre activité militaire est soumise à l'autorisation préalable du commandement. » (art. 24, décret n° 82-598 du 12 juillet 1982).

[128] Ordonnance n° 58-1371 du 29 décembre 1958 tendant à renforcer la protection des installations d'importance vitale, *JORF*, 31 décembre 1958, p. 12064.

[129] Instruction interministérielle n° 4600/SGDN du 8 février 1993 (diffusion restreinte) citée *in* Philippe Burlet, « Protection des PMI de haute technologie en période insurrectionnelle », *Défense, n° 65, septembre 1994, p. 58.*

Relèvent de cette réglementation les sites civils ou militaires considérés comme vitaux pour la sauvegarde de la capacité nationale de réaction à une agression. À côté des sites militaires (tous déjà protégés par leurs propres moyens, comme nous l'avons vu), plus de 2.500 sites civils sont classés points sensibles (on y trouve, des installations de télécommunications et de télédiffusion, les centrales électriques, nucléaires ou non, les oléoducs, certains axes de transport, des gares, des ports, des stocks alimentaires ou de matières premières, des hôpitaux, certaines industries ou services publics, ...) [130]. Toutes les entreprises ou organisations, désignées par leur ministère de tutelle sur proposition des préfets, sont *« tenues de coopérer à leurs frais (...) à la protection desdits établissements, installations et ouvrages contre toute tentative de sabotage »* [131].

Cette protection de points sensibles civils comporte des points communs avec celles des établissements militaires : protection périmétrique et contrôle des accès, établissement d'un plan particulier de protection transmis aux autorités [132], inspections régulières par les services de sécurité et surveillance périphérique exercée, d'une part par les unités de gendarmerie (dans le cadre de leur mission générale de sécurité du territoire) et, spécifiquement, par la DST, service de contre-espionnage responsable de la détection des menaces externes pesant sur les points sensibles.

Même si, au quotidien, la sécurité de ces nombreux points sensibles laisse parfois à désirer [133] et si la protection du secret n'est pas, là, la préoccupation principale, il est clair, cependant, que les mesures préventives prises pour assurer la protection du point sensible contre de possibles atteintes extérieures ne peuvent que renforcer la sécurité des éventuelles informations classifiées qui pourraient s'y trouver.

Cette réglementation des points sensibles comprend plusieurs niveaux de protection suivant la sensibilité du site concerné : RS, PS 1, PS 2, PS 3, ou – au maximum – IPD (Installations prioritaires de défense) [134]. Les *« installations prioritaires de défense »* sont des sites dont, au sens de l'article 17 de l'ordonnance du 7 janvier 1959 [135], les conditions de sécurité sont définies en Conseil de défense. Cette qualification permet notamment de créer des secteurs de sécurité autour de ces installations, secteurs dans lesquels les fonctions de renseignement et de police sont spécifiquement

---

[130] Pour une description d'ensemble, cf. P. Péan, *op. cit.*, pp. 145 à 147.

[131] Article 1er, alinéa 2 de l'ordonnance du 29 décembre 1958, *op. cit.*, p. 12064.

[132] Cf. G. Herrmann, *op. cit.*, p. 89.

[133] La presse révèle régulièrement des informations peu rassurantes sur la protection de certains points sensibles civils. Citons, à titre d'exemple, le Centre spatial guyanais de Kourou, dans lesquels des commandos en exercice se sont plusieurs fois infiltrés à l'intérieur de la base : la Légion, en 1984 (cf. *Le Figaro*, 20 août 1985), le GIGN et le 2e REP, en 1986 (cf. *L'Express*, 11 mai 1990), ou plusieurs installations électriques d'EDF (trois attentats écologistes limités contre des lignes à haute tension, cf. *Le Canard Enchaîné*, 18 avril 1990, puis l'infiltration et un simulacre de sabotage par un commando de la DGSE à la centrale nucléaire du Bugey, cf. *Le Canard Enchaîné*, 25 avril 1990, *Le Monde*, 27 avril 1990 et enfin, un attentat à la roquette contre le surgénérateur Superphenix de Creys-Malville en juillet 1992).

[134] Selon les dispositions de l'instruction interministérielle 4600, le Premier ministre est responsable du classement d'un site aux niveaux IPD, PS 1 ou PS 2 alors que le niveau PS3 relève de la compétence du préfet de département (cf. « Protection des PMI de haute technologie en période insurrectionnelle », *Défense*, n° 65, septembre 1994, p. 58).

[135] L'ordonnance de 1959 a été complétée sur ce sujet, par la loi n° 72-1149 du 23 décembre 1972.

coordonnées en cas de menace conformément aux dispositions du décret du 1er mars 1973 [136].

La protection des zones dédiées à la préservation du secret ou du patrimoine

La conservation en toute sécurité d'informations secrètes nécessite, dans de nombreux cas, de délimiter des zones réservées à l'intérieur des locaux de l'organisme qui en a la charge, et ce notamment dans les entreprises ou les centres de recherche qui, par nature, sont plus sujets au passage de personnes extérieures que les services dépendant directement du ministère de la défense. De même, cet impératif de protection du secret et du patrimoine national scientifique et technique (particulièrement en ce qui concerne les visites et les stages) a conduit à faire de certains sites des *« établissements à régime restrictif »*.

Les zones « réservées » et les zones « protégées »

Les règles de protection du secret exigent, à partir du niveau *Secret défense*, que soit délimitée, à l'intérieur du site une zone, munie de moyens de protection suffisants et d'un système de contrôle d'accès, à l'intérieur de laquelle les documents classifiés seront rédigés, traités et entreposés [137]. Si l'instauration de ce type de zone est obligatoire pour tout service traitant des informations classifiées de ce niveau, le non-respect de cette règle (par exemple, absence de zone, conservation de documents classifiés hors de cette zone, pénétration d'une personne non autorisée, ...) ne constitue, en elle-même, qu'une violation d'une mesure réglementaire interne, ne pouvant donner lieu qu'à une sanction disciplinaire (cf. supra). Il n'y a qu'en cas de compromission d'un secret suite à cette violation – entraînant l'ouverture d'une information judiciaire – qu'une sanction pénale pourrait s'appliquer à ses auteurs (sur le fondement, notamment, des articles 413-10 à 413-12).

C'est donc afin de pouvoir sanctionner pénalement le simple fait de pénétrer dans une zone mise en place dans le but de préserver le secret de défense, que le législateur est intervenu en 1972 pour compléter le Code pénal sur ce point. Souhaitant *« donner un caractère plus impératif »* à l'interdiction de pénétrer dans les zones réservées aux informations classifiées, il avait introduit dans le Code pénal, par la loi du 5 juillet 1972, un article 418.1 qui permettrait à l'autorité ministérielle d'ériger une zone réservée en *« zone protégée »* spécialement visée par le Code pénal [138].

---

[136] Décret n° 73-236 du 1er mars 1973 relatif aux secteurs de sécurité des installations prioritaires de défense, JORF, 7 mars 1973. Par ailleurs, des aires spéciales de surveillances (ass) peuvent être mises en place autour de ces installations afin de faire l'objet de mesures de surveillance phyisques renforcées (cf., notamment, *Armées d'aujourd'hui*, n° 116, *op. cit.*, p. 36).

[137] Cf. A.-L. Mie, *op. cit.*, p. 174.

[138] Cf. P. Péan, *op. cit.*, p. 67. Signalons que l'intrusion sans autorisation dans une zone protégée constituant donc un délit, les mêmes possibilités d'appréhension en *« flagrant délit »* des intrus que celles évoqués plus haut en ce qui concerne les établissements militaires, y sont applicables (et peuvent être utilisées, par exemple, par des agents privés de gardiennage chargés de surveiller la zone).

Cet article visait à donner un fondement légal et à assurer une sanction pénale à l'obligation faite par l'instruction 2000 aux titulaires de marchés classés de créer au sein de leur entreprise une zone protégée destinée à recevoir les informations classifiées et dans laquelle ne pourrait pénétrer que des personnes habilitées [139].

Le décret du 27 mars 1973 [140] précisa le fait que toute zone protégée ne peut être créée que par arrêté ministériel et que, lorsqu'elle a pour objet de protéger des secrets de défense, les autorisations d'y pénétrer sont également délivrées par le ministre ayant créé la zone.

Lorsque le degré de sensibilité des informations ou des activités concernées le nécessite, l'autorité réglementaire a prévu la possibilité de renforcer la sécurité physique des zones protégées en les érigeant en *« zones sensibles »*. Dans les *« zones militaires sensibles »*, les militaires peuvent notamment procéder – après les sommations d'usage – à l'ouverture du feu à l'encontre d'intrus [141]. Plus récemment, un décret de 1985 a permis de créer, sur le même modèle, des *« zones civiles sensibles »* dans les entreprises intéressant la défense nationale (par exemple, entreprises d'armement) : leur protection est assurée *« notamment par des dispositifs dangereux, permanents ou temporaires »* et elles sont signalisées par des panneaux portant la mention *« Défense de pénétrer – danger de mort »* [142].

L'entrée en vigueur du nouveau Code pénal n'a pas modifié profondément ce dispositif. Le nouvel article 413-7 nCP a remplacé l'article 418-1 mais conserve un esprit et une rédaction très proches :

> *« Est puni de six mois d'emprisonnement et de 50.000 F d'amende le fait, dans les services, établissements ou entreprises, publics ou privés intéressant la défense nationale, de s'introduire, sans autorisation, à l'intérieur des locaux ou terrains clos dans lesquels la libre circulation est interdite et qui sont délimités pour assurer la protection des installations, du matériel ou du secret des recherches, études ou fabrications ».*

Sur la base de cet article 413-5 nCP, le décret du 29 mars 1993, déjà cité, abrogea le décret du 27 mars 1973 portant application de l'ancien article 418-1 et le remplaça par les articles R. 413-1 nCP à R. 413-5 nCP. Eux aussi, reprennent quasi textuellement les anciennes dispositions du texte précédent.

Les établissements à régime restrictif

Les différents modes de protection évoqués jusqu'à présent (régime des établissements militaires, point sensible, zone réservée, zone protégée, voire zone – civile ou militaire – sensible) visent, en résumé, à ce que ne pénètrent dans ces sites que des personnes dûment autorisées et à en interdire l'accès aux intrus. Mais il existe, notamment dans les secteurs

---

[139] Cf. Charles Ribière, « Entreprises publiques ou privées intéressant la Défense nationale - Circulation interdite », *Jurisclasseur Pénal*, art. 418.1.

[140] Décret n° 73-389 portant application de l'article 418-1 du Code pénal, *JORF*, 4 avril 1973.

[141] Cf. *Armées d'aujourd'hui*, n° 116, *op. cit.*, p. 28.

[142] Décret n° 85-1357 du 18 décembre 1985 portant création de zones civiles sensibles à l'intérieur de certaines installations d'importance vitale, *JORF*, 22 décembre 1985, p. 15012.

technologiques et industriels, une situation intermédiaire fréquente : celle des personnes extérieures souhaitant pénétrer temporairement sur le site pour des visites ou des stages.

L'ouverture internationale de la France fait que ses entreprises et organismes de recherche sont l'objet de nombreuses visites et stages de la part de personnes de nationalité étrangère (on a dénombré ainsi 30.000 stagiaires et 50.000 visiteurs étrangers en 1985 [143], 41.000 stagiaires et 36.000 visiteurs en 1987 [144] et pour 1992, 50.000 stagiaires [145]). Or, certains exemples ont montré que cet afflux d'intérêt pour nos principaux centres de développement technologique et scientifique n'était pas toujours innocent et recelait souvent des tentatives d'espionnage de la part de services ou d'officines de renseignement étrangers [146]. Une réglementation existe donc pour tenter de filtrer les demandes de visites et de stages de personnes étrangères dans un certain nombre d'établissements considérés comme sensibles. Elle a été définie par une instruction interministérielle sur la protection du patrimoine scientifique et technique français dans les échanges internationaux n° 486 en date du 25 août 1982 et qui a fait l'objet d'une refonte en date du 1er mars 1993 [147].

Son principe consiste, d'abord, à établir et à tenir à jour une liste des *« établissements à régime restrictif »* (complétée par une seconde liste d'établissements moins sensibles, dits *« à accès surveillé »*) ainsi que celle des *« pays soumis à réglementation spéciale »* (c'est-à-dire dont les nationaux font l'objet d'une attention particulière en cas de visite ou de stage) [148]. Ces listes – non publiées – sont arrêtées par le Premier ministre (SGDN) sur proposition des ministres de tutelle et du Conseil d'action scientifique de défense [149]. Parmi ces établissements à régime restrictif, l'on trouverait une centaine de laboratoires de recherche civils [150], les établissements de la DGA, les entreprises travaillant sur des marchés classés de défense et tous les établissements soumis à la réglementation des points sensibles (cf. supra).

Tout établissement à régime restrictif est, dès lors, tenu de soumettre à autorisation préalable les projets de visites et de stages de nationaux étrangers. L'autorisation doit être donnée au niveau du ministère de

---

[143] Chiffres cités par la Direction de la Surveillance du Territoire in « Visiteurs et stagiaires étrangers dans nos entreprises et laboratoires - une coopération pas toujours innocente... », *La Jaune et la Rouge*, août-septembre 1987, p. 84.

[144] Chiffres cités par la Direction de la Surveillance du Territoire in *Réalités Industrielles/ Annales des Mines*, octobre-novembre 1989, p. 61.

[145] Estimation du SGDN cité par *Valeurs Actuelles*, 27 décembre 1993, p. 4.

[146] Cf. notamment *La Jaune et la Rouge*, *op. cit.*, pp. 83 à 86; l'interview du général de Barry (alors SGDN) : « Les limites du secret scientifique », *La Recherche*, n° 151, janvier 1984, pp. 123 à 127; plus récemment Pierre Louisot, « Protection du patrimoine scientifique » *INSERM Actualités*, n° 122, janvier-février 1994, p. 10; et pour un exemple révélé par la presse : « La France fournissait aussi de la matière grise à l'Irak », *Le Canard Enchaîné*, 20 février 1991.

[147] Pour une courte synthèse de ce texte, cf. SGDN, *Bulletin de sécurité de défense*, n° 9, janvier 1995, p. 2; cf. également Michel Ferrier, « Technique, défense nationale et technologie » in Raymond Bloch (dir.) *Ethique et société - Les déontologies professionnelles à l'épreuve des techniques*, Institut Fredrik R. Bull, Armand Colin, 1997, pp. 126-129.

[148] Cf. J. Huygues des Etages, *Avis de la commission de la défense nationale sur le budget pour 1984*, Assemblée nationale, 1re session ordinaire 1983/1984, séance du 6 octobre 1983, document n° 1738, fiche n° 8, p. 35.

[149] Cf. *La Recherche*, *op. cit.*, p. 124.

[150] *Idem*, p. 123.

tutelle (représenté par le Haut fonctionnaire de défense), sauf délégation de pouvoir donnée dans certains cas à des autorités subordonnées, voire aux responsables des sites. Le SGDN n'est consulté que pour les autorisations

> *« qui concernent les cas les plus délicats remontant au niveau du Premier ministre (10 % environ). En moyenne, sur 2.500 dossiers traités annuellement à ce titre, le pourcentage de refus total est inférieur à 5 %, et environ 20 % font l'objet d'une réorientation ou de refus partiels. »* [151]

Lorsqu'une visite ou un stage est autorisé dans un établissement à régime restrictif, il appartient cependant au responsable de ce site et aux personnes qui y sont en charge de la sécurité de faire en sorte que le circuit de visite ou le lieu d'affectation du stagiaire ne risque pas d'amener la personne étrangère au contact d'informations classifiées ou à pénétrer à l'intérieur d'une éventuelle zone réservée ou protégée.

Malgré ces précautions, il semble que la protection du patrimoine scientifique et technique national assurée au sein des sites de recherche eux-mêmes reste peu efficace et devra évoluer dans son principe et dans ses moyens [152].

---

[151] *Idem*, p. 126.

[152] Michel Ferrier, directeur du pôle Technologie et transferts sensibles du SGDN reconnaît lui-même les difficultés auxquelles une telle politique de protection est exposée : *« Devant cette impossibilité de contrôler les conséquences de ces coopérations* (scientifiques et techniques avec des partenaires étrangers) *devenues trop nombreuses, il a alors été envisagé de faire porter le diagnostic d'opportunité en termes de sécurité, sur la coopération elle-même. Tel est le sens, depuis 1993, de la circulaire du Premier ministre. Mais le monde de la recherche, qui avait été pourtant consulté, n'a pas pleinement compris que soit substitué le contrôle des thèmes de coopération au contrôle des coopérants. Ce fut sans doute une maladresse de heurter la sensibilité scientifique là où elle se sentait complétement propriétaire... Cependant, l'abandon de tout contrôle supposerait que l'on pût faire appel, par une action de sensibilisation, au sens de la responsabilité des universitaires et des scientifiques en matière de sécurité, c'est-à-dire dans un domaine qui leur est peu familier et pour lequel ils éprouvent, en France tout au moins, une répulsion instinctive et héréditaire »* (M. Ferrier, *op. cit.*, p. 128).